COMPUTER CRIME

HANDOUTS AND HINTS

Special Agent in Charge Peter F. Roe
Amtrak Police Department
Fraud/Organized Crime Unit

COMPUTER CRIME

HANDOUT AND HINTS

Special Agent in Charge Peter F. Moe
Amtrak Police Department
Fraud/Organized Crime Unit

Overview of Computer Crime: Carlton Fitzpatrick

Relevant Federal Statutes:

Categories of Computer Crime

Raiding The Computer Room - Fourth Amendment
Considerations: John Gale Sauls

Computer Crime Investigation Techniques: Wayne Cerow

Evidence Considerations In Data Processing Investigations

Other Technical Investigative Techniques -

- Mail Covers
- Electronic Mail and Data Transmission
- Recording Data Communications
- Planning A Data Processing Investigation
- Computer Matching: Kusserow
- Identifying "800" Telephone Access Numbers

Sample Affidavit For Search Warrant

Computer Crime Digest

Overview of Computer Crime

Moderator:
CARLTON W. FITZPATRICK
Computer and Economic Crime
Branch
Federal Law Enforcement Training
Center
Glynco, GA

Remarks by Carlton W. Fitzpatrick

My objective is to clarify some issues relating to computer crime, and to dispel some long-standing misconceptions held by both law enforcement and the general public.

Specifically, I wish to address four separate topics: the pervasiveness of computer crime; the various roles of computers in economic crime; primary methodologies of computer crime; and the role of law enforcement agencies in dealing with computer related crime.

The Pervasiveness of Computer Crime

When one considers that virtually all businesses, regardless of size, utilize computers to some degree, a couple of sobering facts emerge. First, computer crime is within the capability of millions of people, much more than most of us realize. Second, most computer crime is, therefore, within the investigative jurisdiction of state and local agencies.

Large organizations, with their multi-million dollar revenues and mind-numbing computer power, have the resources to hire a small army of computer auditors and data security personnel to protect the integrity of their system. Users of small business systems, microcomputers, and [illegible] have limited resources and cannot afford full-time data processing professionals. They must rely on the generic security systems which were purchased with their small systems. Managers and owners of these machines are not educated to the symptoms of computer crime, so controls may be virtually non-existent.

Davis Publishing Company
Police Division
37 YEARS OF PROVEN SUCCESS IN ASSISTING LAW ENFORCEMENT PERSONNEL IN PROMOTIONS

and the chances of undetected computer crime are quite high.

Computer crime is a significant problem that is not likely to diminish. Some of the earliest research in this area was conducted by the Stanford Research Institute. They can be credited with first raising this issue before the national conscience. More recently, the American Bar Association, the American Institute of Certified Public Accountants, and the President's Council on Integrity and Efficiency have examined the degree of computer crime. Although few, if any, of these works were based on solid empirical data, each of them served to broaden the awareness of the American public, the press, and law enforcement agencies. Computer-related crime is a multi-billion dollar problem.

Roles of Computers In Economic Crime

One of the difficulties encountered by researchers in the aforementioned projects was in developing a workable definition of computer-related crime. Being a law enforcement officer and not a researcher, I define computer crime as any crime in which a computer plays some role, actively or passively. This broadens the horizon of our discussion, but at the same time enables us to look at important examples which researchers might tend to overlook.

I see computers playing four distinct roles in economic crime: a) as a passive partner; b) as the object of the crime; c) as a tool of the crime; and d) as an intimidating symbol.

Passive involvement of computers. In these types of crimes, the computer, while not being directly involved in the scheme, is part of the working environment. The crimes may be rather traditional schemes such as contract fraud or accounting fraud, and the computer may do little more than to serve as a pipeline for correspondence, memos, accounting reports, and other typical office transactions.

We should remember, though, that modern computers have an almost procreational tendency to create files. These files, many of them transient, will be stored in the system's disk facilities and many times forgotten. Virtually all sizable systems are backed up daily onto an inexpensive medium such as magnetic tape and filed away as insurance against future disk or file failures. Dormant files eventually become archived onto tapes.

This means, of course, that there are reels of magnetic tapes scattered throughout corporate America. Buried within these tapes are long-forgotten files dealing with correspondence, directives, and other historical accounts of interest to the investigative agencies. When written documents of suspected fradulent activities are unavailable, remember the computerized versions of these written documents, which may be stored internally within the organization's computer or externally on tapes or other storage media.

Computers as objects of criminal activity. One of the most pervasive types of computer crime is the one where the criminal directs his criminal activity toward the computer itself, or rather at the information internally stored within the computer. There are generally four things an unscrupulous individual may wish to do to a computer: add, delete, modify, or scan computer data.

There are hundreds of examples of relatively low-paid, data-entry personnel inputting phony data into a system. Phony records may be added to an accounts receivable system, non-existent people to a payroll system, or unauthorized verifications to a payment system. The potentials are limitless. Frequently they have the foresight to cover their trail with necessary paperwork, such as phony invoices or vouchers, but generally speaking they rely on the sheer volume of records processed by the computer to bury criminal activity.

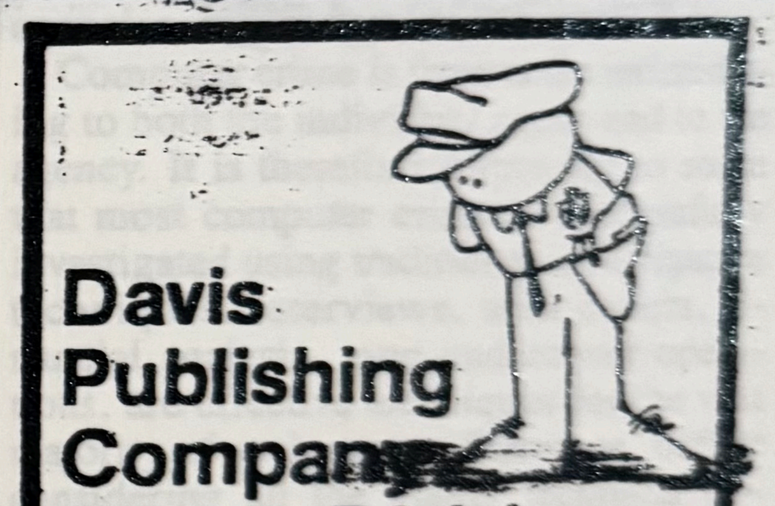
Just as phony data can be added to a system, legitimate data can be deleted. Some examples are bad credit ratings removed from credit bureau records, accounts payable records purged, and others.

Many low-level data conversion clerks do not have the authority or the ability to add and delete records. Many, though, have authority to change existing records. The result can be just as fraudulent. Salaries can be increased without authorization in payroll systems. In inventory systems, dates of purchase can be altered so that brand new merchandise will be immediately surplussed as outdated materials. There are countless variations of this very common practice.

Much of the data stored on our national computer system is intelligence. To the would-be criminal there may be no desire to input, delete, or alter anything; just to scan it. Such records may pertain to national security data, corporate or trade secrets, contract bids, etc. Certain information in the wrong hands can be devastating.

Computers as tools of criminal activity. The criminal underworld has discovered the glories of microcomputers. Electronic spreadsheets keep fast and accurate records of accounts owed. Statistical packages calculate gambling odds and help regulate numbering rackets. With the recent cost-effective developments of disk encryption packages, law enforcement agencies are being prodded into finding new investigative techniques. Microcomputers also are excellent tools for penetrating larger systems. The press has flooded us with horror stories of how people with inexpensive home computers and a modest knowledge of telecommunications have plagued the corporate and governmental computer systems of the nation. Armed with new statutes, both at the federal and state levels, law enforcement agencies are beginning to fight back with encouraging results.

Computers as items of intimidation. Millions of people believe that computers don't make mistakes. Even if they did, you can't communicate with data processing folks. They speak a strange language and make you feel stupid for asking questions. Therefore, the safest thing to do emotionally and mentally is simply accept unquestionably. Several years ago numerous



Davis Publishing Company
Police Division

37 YEARS OF PROVEN SUCCESS IN ASSISTING LAW ENFORCEMENT PERSONNEL IN OBTAINING PROMOTIONS.

For a FREE Catalog
CALL: 1-800-221-2040
P.O. Box 17359,
Montgomery, AL 36117

Circle no. 10 on Reader Service Card

insurance underwriters purchased millions of dollars in phony insurance policies from the Equity Funding Corporation, perhaps with this same viewpoint that, if the printouts came from a computer, they must be right. This attitude may be the most pernicious aspect of the so-called computer generation.

Methodologies of Computer Crime

There are as many ways of perpetrating computer crime as there are personalities and imaginations. We can break these methods down into three general areas: non-technical schemes; those schemes requiring at least a modicum of computer skills; and those high-tech crimes requiring extensive computer, technical or engineering skills.

A common misconception is that computer crime is the sole domain of brilliant, well-educated technophiles who, by their sheer knowledge, are masters of any computer system. The fact is that by far the majority of computer crimes are perpetrated by relatively low-paid, non-skilled persons with only a moderate education. These people do, however, have two significant traits: they know the role that the computer plays within the organization, and they have access to the computer.

Most computer crime, at least when measured by the number of instances and not the amount of money involved, is perpetrated by insiders. Supposedly, for every dollar that an organization loses to outside thieves, it loses three dollars to its own employees. If anything, computers serve to widen these figures.

Password theft is rather common and is at the root of many crimes. Basically, the password is the individual's key to certain areas of the computer's filing system. One's password or other access code gives the user all the privileges of the true owner, including the ability to access restricted files, alter file contents, and so on. Some intriguing schemes for stealing passwords have been developed.

Non-technical personnel may possess the skills and attributes necessary to perpetrate significant fraud. As plentiful as these types of crimes are, they are relatively easy

puter skills are associated with computer program manipulation. Programs are the instructions that tell the computer what to do with the incoming data. Since programming is a career that requires some education, it stands to reason that one must have some level of technical skill to alter these instructions.

Data processing professionals use the term "Trojan Horse" to refer to a maliciously altered program. It may require only a line or two of malevolent entries to totally destroy the integrity of the system. Since these alterations are buried within thousands or millions of other entries, they may be extremely difficult to detect. The perception is that the program is functioning normally, whereas in reality it will, when the malicious entry is encountered, perform illicit tasks it was not originally designed to perform.

A "trap door" is a particular type of program modification that has proved enormously difficult to detect, simply because the computer works well most of the time. Simply stated, the programmer inserts a line of code instructing the computer that when certain conditions are met, an illicit routine is initiated. When the program is tested for legitimacy, the trap door will not be detected unless those unique conditions are inadvertently met. For example, a trap door in a payroll program would be that, when employee A's pay records are processed, the program prints a duplicate check, makes no log entry of the check being printed, then loops back to the regular routine and continues to function as normal.

These crimes are harder to detect. When detected, they create investigative problems for the agency. It is generally recommended that, when these types of intermediate schemes are investigated, the assigned agent should have some degree of familiarity with data processing principles. He or she must be able to communicate with the technical personnel and comprehend the organizational and technical structure of the environment. Incidences of these types of crime are not so numerous as the non-technical crimes, but they extend over a longer period of time and involve greater financial losses.

The most difficult cases for law enforcement agencies are those involving individuals with considerable technical skills. These high-tech crimes are relatively rare, but may involve enormous sums of money

crime. After all, the agent is a professional law enforcement officer, not a technician. Therefore, the agent should know where to go to get expert assistance.

A few of these sources would be: the data processing staff of the individual agency; the local technical university and its computer science staff; other colleges that are involved in teaching computer courses; user groups or professional organizations; the vendor of the suspected computer or software system; and private contractors.

The Role of Law Enforcement Agencies In Computer Crime Investigations

A generally accepted rule is that every agency responsible for financial crime investigations should have the ability to investigate such crimes. Moreover, it is safe to say that any financial investigator should have the ability to investigate non-technical types of computer crime. Many small agencies may have financial investigative responsibility, but lack the resources to adequately conduct investigations. In such instances, close liaison should be maintained with state or county agencies.

Computer crime is frequently intimidating to both the individual agent and to the agency. It is therefore surprising to some that most computer crime is successfully investigated using traditional investigative techniques. Interviews, mail covers, financial analysis, even undercover operations, are effective techniques for the vast majority of such cases. Therefore, before considering all the highly technical options in computer crime investigations, we should first look at the tried and true methods to see if they are applicable to the present situation.

It is important to note that most computer thieves are amateur criminals. Being so, they frequently make amateurish mistakes, like talking too much or mishandling the gains of their deception. Since most law enforcement officers are trained to deal with professional crooks, dealing with amateurs is sometimes much easier than one might expect. The computer crook often depends on lack of detection to get away with the crime. When the crime is detected, there may be few possible suspects and even fewer places for the

conduct competent investigations of the intermediate or more technical nature. The foundation for such an assignment should be a thorough knowledge of financial in-

vestigative techniques and an interest in computers. Training alone is not the answer to developing good computer crime investigators. As in most areas, computer fraud investigative training only lays the groundwork. The true education comes from participating in such investigations. Credibility comes from training and experience.

In complex cases involving computers, the abilities of one agent will not be sufficient. A team approach to the investigation is recommended. A solid investigative plan should be established early in the investigation, and a determination made of available resources and jurisdiction.

It is a misconception that computer crime is primarily the concern of the federal government. The fact is that the vast majority of instances of computer crime are within the jurisdictions of state and local agencies.

Computer crime is here to stay. Law enforcement is doing an admirable job in combatting it, considering all the legal and technical hurdles that must be overcome during an investigation and prosecution. Agencies cannot slacken in their commitment to develop expertise in computer-related investigations. The future of law enforcement depends heavily on our commitment to stay abreast of current and developing criminal trends.

RELEVANT FEDERAL STATUTES

I. COMPUTER FRAUD AND ABUSE ACT OF 1986 (18 U.S.C. 1030)

A. Unauthorized access to obtain national defense, foreign relations, or restricted data

B. Unauthorized access to obtain financial institution, card issuer, or credit information

C. Unauthorized access of federal computer affecting operation.

D. Accessing federal interest computer with intent to defraud

E. Alteration, damage or destruction of information in federal interest computer.

II. THEFT AND RELATED STATUTES

A. 18 U.S.C. 641 (Embezzlement or theft of public money, property, or records)

B. 18 U.S.C. 659 (Theft of goods or chattels moving as, which are a part of, or which constitute interstate commerce)

C. 18 U.S.C. 2314 (Interstate transportation of stolen property)

D. Miscellaneous Theft and Theft-Related Offenses

1. 18 U.S.C. 654 (Federal employee who wrongfully converts the property of another which is entrusted to him)

2. 18 U.S.C. 2315 (Receipt of goods stolen from interstate commerce)

III. ABUSE OF FEDERAL CHANNELS OF COMMUNICATION

A. 18 U.S.C. 1341 (Mail Fraud)

B. 18 U.S.C. 1343 (Wire Fraud)

IV. TRESPASS AND BURGLARY

A. 18 U.S.C. 2113(a) (Banks)

B. 18 U.S.C. 2115 (Post offices)

C. 18 U.S.C. 2117 (Interstate carrier facilities)

V. DECEPTIVE PRACTICES

A. 18 U.S.C. 912 (Obtaining thing of value by impersonating an officer or employee of the Unit States)

B. 18 U.S.C. 1001 (False statements)

C. 18 U.S.C. 287 (False claims)

D. 18 U.S.C. 1005, 1006 (False entries in records of banks and credit institutions)

VI. PROPERTY DAMAGE

A. 18 U.S.C. 81 (Arson)

B. 18 U.S.C. 1361,1363 (Malicious injury)

VII. MISCELLANEOUS PROVISIONS

A. 18 U.S.C. 1905 (Disclosure of confidential information)

B. 18 U.S.C. 701 (Unauthorized use of identificatio

CATEGORIES OF COMPUTER CRIME

1. TYPE I - INPUT/OUTPUT FRAUD
   - A. Data Diddling
   - B. Record Adds/Deletes
   - C. Source Document Tampering
   - D. Impersonation
   - E. Piggybacking
2. TYPE II - PROGRAM/DATA FILE MANIPULATION
   - A. Trojan Horse/Trap Door
   - B. Scavenging
   - C. Salami Slicing
   - D. Foibles
   - E. Browsing
3. TYPE III - O/S PENETRATION/COMMUNICATIONS
   - A. O/S Alteration
   - B. Superzapping
   - C. Time Bombs
   - D. Wiretapping
   - E. Interception

Raiding the Computer Room
Fourth Amendment Considerations (Part I)

"Computer-related crimes present new challenges in the establishment of probable cause...."

By
JOHN GALES SAULS
Special Agent
FBI Academy
Legal Counsel Division
Federal Bureau of Investigation
Quantico, VA

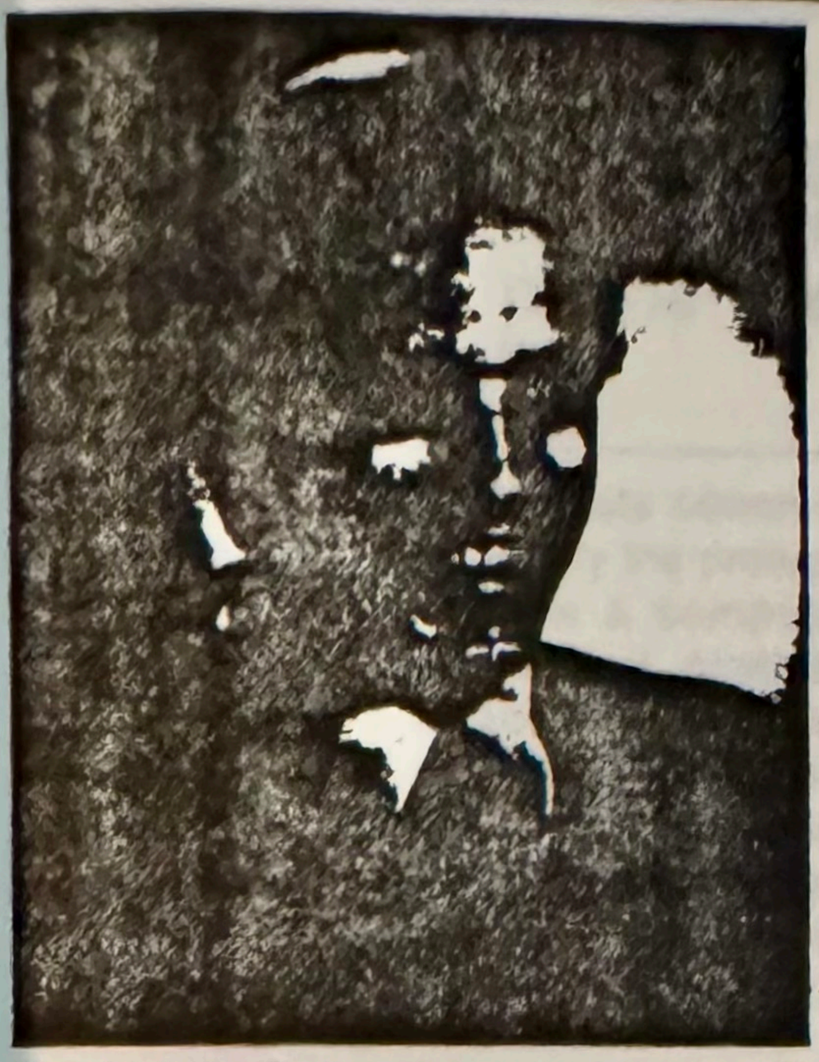
Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

For several decades, electronic computing machines have been changing the world. Businesses now record their activities by computer, law enforcement agencies maintain criminal records by computer, children are entertained by computer-driven electronic games, and authors process their words by computer. Even tasks such as medical diagnoses are being performed with the aid of computers.

In the last decade, the proliferation of low-cost "home computers" has facilitated the spread of computer power and knowledge to vast numbers of citizens. Thus, it should be no surprise that criminals have begun to use computers to commit crimes and to record the activities of their criminal enterprises. Consequently, law enforcement officers are finding it increasingly necessary to search for, examine, and seize computers and computerized records in successfully investigating and prosecuting many criminal acts.

While conducting investigations of computer-related crimes, officers must comply with an 18th century prohibition against "unreasonable searches and seizures"[1] and contend with 20th century electronic technology. For example, investigators may at times find themselves searching for intangibles rather than familiar physical evidence, such as guns or stolen stock certificates. As one court has noted, the target of a search may be "records [that] exist as electronic impulses in the storage banks of a computer."[2] This new technology creates the possibility of a criminal armed with a home computer in Wisconsin contacting a computer in New York by telephone and illegally causing funds to be transferred electronically to a bank account in France. Regardless of these technological advances, search and seizure by law enforcement officers continues to be governed by the fourth amendment to the U.S. Constitution.[3]

This two-part article will examine issues that arise when officers seek a warrant to search and seize a computer and the information it has processed. Part I will address the application of the fourth amendment warrant requirement to computer-related searches, focusing on special problems officers may encounter in establishing probable cause to search and particularly describing the computer equipment to be seized. Part II will address the description of computer-processed information to satisfy the particularity requirement and then consider issues that may arise in the execution of a warrant authorizing the seizure of a computer and computer-processed information.



Special Agent Sauls

WARRANT REQUIREMENT

The fourth amendment protects the right of the people to be "secure in their persons, houses, papers and effects" against unreasonable Government intrusion.[4] This protection extends to computers, which are effects, and to information processed by this electronic technology, which can be categorized as papers. The constitutional demand upon the officer seeking to seize a person's computer or computerized information is that the seizure be reasonable.[5] The U.S. Supreme Court, in establishing guidelines for reasonable searches and seizures, has stated a preference that they be made pursuant to a judicially issued search warrant. The "Constitution requires that the deliberate, impartial judgment of a judicial officer be interposed between the citizen and the police . . . searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[6] This requirement that a warrant be obtained prior to a search or seizure is applied with special strictness where business or residential premises, the places computers are most likely to be located, must be entered to perform the search.[7]

The fourth amendment sets forth certain procedural requirements that must be met if a valid warrant is to be issued. There must be a showing of probable cause supported by oath or affirmation, and the warrant must particularly describe the place to be searched and the persons or things to be seized.[8] In addition, the Supreme Court has held that the probable cause determination must be made by a neutral, detached magistrate.[9] The requirements of oath or affirmation and of presentation to a neutral, detached magistrate raise no special problems where computer searches are concerned; however, the probable cause and particularity requirements pose unique problems where computers are the search target, and these issues merit discussion.

Probable Cause To Search

Central to the protections provided to citizens by the warrant requirement is the command that no warrants shall issue but upon probable cause.[10] This language has been interpreted to require that before a search warrant may be issued, the Government must set forth facts that would cause a reasonable person to conclude that it is probably true that (1) a crime has been committed, (2) that evidence of that crime is in existence, and (3) that the evidence presently exists at the place to be searched.[11] Obviously, satisfying this requirement necessitates the collection and presentation of information, and law enforcement officers perform this task daily in regard to numerous crimes. Computer-related crimes present new challenges in the establishment of probable cause though, because of the unfamiliar technology involved. Although a magistrate likely already understands how a murder may be committed with a gun, he may require considerable explanation before finding that an embezzlement was committed by means of a computer. The problem is largely an educational one.

Inasmuch as computers may be used in a wide variety of criminal endeavors, ranging from fraud to espio-

"... an officer seeking to convince a magistrate that a novel crime has been committed should use care to ensure that the explanation of the mechanics of the crime is clear and easily understood."

nage, it is difficult to state concisely what is required to satisfy the probable cause requirement in a computer-related crime. In general, probable cause will be established just as it would in a case where no computer was involved, except that additional facts will have to be presented regarding the role of the computer in the criminal activity.

That a Crime Has Been Committed

The first hurdle in establishing probable cause to search is articulating facts to indicate that a crime probably has been committed. In determining what additional facts a magistrate will need to make such a finding where a computer is involved in the crime, it is helpful to examine the role played by the computer in the criminal activity. For example, where a computer is stolen, the crime is the same as any other theft, and the required factual showing, describing the computer as the object of the crime, would likewise be the same. Where a computer is used as a tool to commit a crime, facts must be presented to show the crime was committed and to explain how the computer was used in the commission. Because computer systems are commonly installed so they may be used from distant locations by means of electronic communication over telephone lines, novel criminal opportunities have been created.[12] Valuable data may be transferred from one computer to another or modified to achieve advantage for the computer criminal.[13] Inasmuch as the means used to commit these crimes are unfamiliar, the officer must convince the magistrate that such a crime has been committed by detailing how it was committed.

An example of an officer successfully obtaining a search warrant in a case where new technology was being employed to commit the crime of fraud is found in the case of *Ottensmeyer* v. *Chesapeake & Potomac Telephone Co.*[14] Ottensmeyer, who ran a telephone answering service, decided to provide an alternative to his customers to normal, commercial long-distance telephone service. He found a strategically located town that enjoyed nontoll calling service to a larger city on either side, despite the fact that a call from one of the larger cities to the other was a toll call. Ottensmeyer installed an electronic device in the small town that allowed a customer in one of the large cities to "patch" a call to the other large city through the device, thereby avoiding a toll call and defrauding the phone company of revenues to which it was entitled.

The investigator, a police officer who had special training in electronic technology and telecommunications, sought a warrant to search the premises where the "patching" device was located. In his affidavit, the officer "informed the judge of his experience in the electronic field and of his independent investigation and conclusions."[15] The officer articulated facts that explained how the scheme to defraud functioned, and drawing on his expertise, cited inferences he had drawn from the facts he had observed. The warrant was issued and the search performed.[16]

Obviously, an officer seeking to convince a magistrate that a novel crime has been committed should use care to ensure that the explanation of the mechanics of the crime is clear and easily understood. If the officer wishes the magistrate to consider the officer's interpretations of the facts he has observed, he must inform the magistrate in his affidavit of the experience and training that accredit these interpretations. Consideration of such inferences by a magistrate determining probable cause has been approved so long as the officer sets forth the training and experience upon which they are based.[17]

An officer seeking to establish probable cause where the crime is unusual or unfamiliar may also elect to use the services of an expert. An example of using information provided by experts in affidavits for search warrants is found in *United States* v. *Steerwell Leisure Corp., Inc.*[18] Steerwell was charged with infringing upon the copyrights of a number of electronic video games, and the question of whether a crime had been committed turned on whether the games Steerwell was distributing were sufficiently similar to the copyrighted games to violate the copyright statute. The affidavits to support search warrants presented the magistrate with results of expert analysis in comparing the games distributed by the defendants with the copyright-protected games. In determining the validity of the warrants issued on those affidavits, the court concluded that the magistrate was entitled to accept the conclusions of the experts, but noted the "magistrate's determination of probable cause would be facilitated if the agents' affidavits contained more details concerning the comparisons between protected games and infringing games."[19]

"The primary rule of particularity should be to make the description of the items to be seized as precise as the facts will allow."

The court also made reference to the importance of explaining to the magistrate how the crime was committed, in this case by duplication of the circuit boards that control the action of electronic games.[20] Again, the task of the officer includes providing sufficient technical details in layman's terms to familiarize the magistrate with the mechanics of an unusual crime.

That Evidence of the Crime Exists

The second hurdle for an officer seeking to establish probable cause to search is setting forth facts to convince a magistrate of the probability that evidence of the crime exists. Where a computer is stolen, the stolen computer is evidence of the crime. If the theft is established factually, then the existence of the computer as evidence is likewise established. Similarly, where facts establish that a computer was used to commit a crime, the same facts establish that the computer used was an instrumentality of the crime. This was demonstrated in the *Steerwell Leisure Corp.* case where if the magistrate found that the circuit boards in question violated the copyright laws then the boards would also constitute evidence of that violation.[21]

Where an investigator seeks to establish that computerized records of criminal activity are in existence, his task is essentially the same as establishing the existence of noncomputerized records. He must factually establish that records of the criminal activity have probably been created and retained. There is authority for the position that it is unnecessary to establish factually in the affidavit the physical form in which the records sought are expected to be found.[22] If the officer can establish factually the creation and retention of the records, he need not specify (or know) whether they are being maintained in written, magnetic, or some other form. In *United States* v. *Truglio*, audio cassettes were seized during the execution of a search warrant authorizing the seizure of "... books, records, indices, movies regarding the interstate prostitution operation located at the King of the Road Health Club...."[23] In approving seizure of the audio cassettes, the court noted that "it would have been more precise for the warrant to have specified 'written or electronic records,' " but then stated that "[s]tandards of pragmatism and commonsense must necessarily be adaptable to changing times and technological advances."[24] The court concluded by saying that "[w]hile decades ago it might have been difficult reasonably to infer that records existed in some form other than written, in the mid-1980's commonsense demands that we refrain from remaining so inflexible."[25]

That Evidence of the Crime Presently Exists at the Place to be Searched

Finally, the investigator seeking to establish probable cause to search must factually establish the probability that the evidence sought is presently located at the place he is seeking authorization to search. Whether this requirement of recent information has been met is "... determined by the circumstances of each case."[26] As stated by the U.S. Supreme Court, "[t]he task of the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that ... evidence of a crime will be found in a particular place."[27]

The requirement for recent information is easily satisfied where the investigator can set forth reliable information that the object sought has been recently observed at the proposed search site. Where such facts are not available, other facts must be used to infer that the items to be seized are presently at the place to be searched. At times, having a computer or its records as the target of the search may simplify meeting this requirement. If a computer has been used to commit a crime telephonically, it is possible that it has also been set up to "answer" incoming calls, to allow other computer operators to call it using their computer terminals and a telephone. If such an operation exists, an incoming call will be answered with a tone called a "carrier."[28] When a particular phone is answered with a "carrier," it seems reasonable for a magistrate who has been informed of the significance of the "carrier" to find that a computer and related equipment are probably present at the location of the telephone.

A somewhat analogous case involved a search warrant issued for the seizure of a "blue box," an electronic device used to create tones on the telephone system to facilitate the making of long-distance calls without being billed for the toll charges.[29] In this case, tones such as those produced by a "blue box" had been monitored by the telephone company on a particular telephone for a period of weeks, ending the day prior to the issuance of the warrant. This information was related to the magistrate in the affidavit. In

upholding the validity of the resulting search warrant, the court concluded that "[t]he affidavit set forth substantial information establishing clear probable cause to believe that a device emitting a 2600 cycle tone and Southwestern Bell multifrequency tones was being utilized ... at [the] residence."[30]

Where computerized records are sought, the magistrate should consider that records by their nature are created to be kept for at least a minimum period of time, along with the other facts presented, in determining whether the records are presently at the place to be searched.[31] Although each case must be evaluated on its own facts, the U.S. Supreme Court and lower courts have held that under certain circumstances, it is reasonable to expect that records seen 3 months previously will still be present at that same location.[32]

Particularity

The fourth amendment commands that "no warrants shall issue except [those] ... particularly describing the place to be searched and the persons or things to be seized."[33] This provision requires that a warrant authorize only a search of a specific place for specific named items. Coupled with the probable cause requirement, this provision prevents general searches by ensuring that the warrant describes a discrete, defined place to be searched, describes only items connected with criminal activity for which probable cause has been established, and describes the items so definitely that it removes from an officer executing the warrant the discretion of determining which items are covered by the warrant and which are not.[34] It also provides a signal of when a search is at an end, that is, when all items named in the warrant have been located and seized or when all possible hiding places for items not located have been explored.[35] Since the "place to be searched" portion of the particularity requirement has no special impact on computer searches, it will not be discussed. However, the "things to be seized" portion of the requirement has a marked impact in seeking a warrant to authorize the seizure of a computer or information processed by a computer. This portion will be examined in regard to both the computer and the processed information.

Describing the Computer

The primary rule of particularity should be to make the description of the items to be seized as precise as the facts will allow. A court measuring the particularity of a description in a search warrant may consider what facts could reasonably be known by the investigator at the time application for the warrant was made, so long as the investigator includes all the facts known to him in the affidavit.[36] Consequently, the circumstances of each case can help determine whether a description is sufficiently particular. The nature of the item sought also is considered in determining the degree of particularity required. A less precise description is required of items which are contraband, such as controlled substances.[37] Conversely, greater particularity is demanded when the item sought is of a type in lawful use in substantial quantities.[38] Generally, where computer equipment is sought for seizure pursuant to a search warrant, a quite particular description will be required.

Where a computer has been reported stolen, it is reasonable to expect that the owner will provide a detailed description of the stolen item. Therefore, if the object of the search is a stolen computer, a detailed description, including manufacturer, model number, and serial number if known, will probably be required. This is especially true if the computer sought is a type commonly in lawful use. Care should be taken to ensure all available descriptive information is included.

Where computer equipment is sought because it was used as an instrumentality to commit a crime, the most precise description the facts will allow may be a more general one.[39] Where a victim complains that his computer system has been accessed telephonically by an unknown person and a loss has resulted, it is likely that the investigator will only be able to determine generally what types of devices were used to accomplish the crime. He may, for example, learn that a computer terminal (a keyboard and display monitor) and a modem (a device that allows digitally encoded computer information to be transmitted over telephone lines) were necessary to perform the acts accomplished, but will have no information regarding the manufacturers of the equipment, model numbers, or serial numbers. If a telephone trace reveals the location from which the intruding call originated, the investigator may have probable cause to search. Under these circumstances, the general description of "a computer terminal and a modem of unknown make or model" may suffice.

An analogous case is *State* v. *Van Wert*,[40] where police had probable cause to believe Van Wert was using equipment to forge checks. A search warrant was issued authorizing the seizure of "check protectors and typewriters used in preparation of forged checks." The court approved use of this general language based upon the nature and information known con-

"Where a computer is used as a tool to commit a crime, facts must be presented to show the crime was committed and to explain how the computer was used in the commission."

cerning the crime, stating that greater particularity "... was not needed in this case where defendant was under investigation for forgery rather than theft of a certain item."[41]

Similarly, the warrant in *United States* v. *Harvey* authorized the seizure of "a 'blue box,' an electronic device that allows a caller to make long distance calls without them being recorded for billing by the telephone company."[42] The Agents executing this warrant ultimately seized audio cassette tapes that had tones such as those produced by a "blue box" recorded on them. The court noted that the affidavit clearly established that a device emitting "blue box" type tones was being used at the place to be searched and then addressed the particularity question, observing that "[n]either the Southwestern Bell officials nor the FBI Agents knew the actual physical form which the device would take, and they assumed it would be in the form familiar to their research and experience...."[43] The court, in approving the seizure, said, "[t]he cassette tapes constituted 'an electronic device that allows a caller to make long distance phone calls without them being recorded for billing by the telephone company' and were thus properly seized as within the limitations of the warrant."[44]

Since computer systems are often comprised of a number of component parts,[45] an investigator applying for a warrant to seize a computer should ensure that the warrant describes all parts of the computer system that are probably present, as well as the various types of storage devices upon which the machine's operating instructions (computer programs) are maintained. It is prudent to consult an expert concerning the items to be listed. Equipment components will probably include a central processing unit, printers, terminals (keyboards and display screens), magnetic tape drives, and magnetic disc drives. Storage media will include magnetic tapes, magnetic discs, punched cards, and paper tapes. Computer printouts will also likely be present.[46] If information that has been processed is being sought, it is especially important to particularly describe the storage media. Consultation with an expert will increase the likelihood of a thorough listing of the items of evidence probably present, and provided the expert's education and experience are set forth in the affidavit, will give the magistrate a sound basis for concluding that the items sought are probably located at the place to be searched.

Part II of this article will conclude the particularity analysis and discuss problems with executing this type of search warrant.

FBI

Footnotes

[1] U.S. Const. amend. IV.
[2] *United States* v. *Hall*, 583 F Supp. 717, 718 (E.D. Va. 1984).
[3] *See Katz* v. *United States*, 389 U.S. 347 (1967).
[4] U.S. Const. amend. IV.
[5] *See Katz* v. *United States*, 389 U.S. 347 (1967).
[6] *Id.* at 357.
[7] *See Michigan* v. *Tyler*, 436 U.S. 499 (1978).
[8] U.S. Const. amend. IV.
[9] *Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971).
[10] U.S. Const. amend. IV.
[11] *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 556–557 n. 8 (1978), quoting Comment, 28 U. Chi. L. Rev. 664, 667 (1961).
[12] For a discussion of computer telecommunication crime, see Marbach, "Beware: Hackers at Play," *Newsweek*, September 5, 1983, p. 42.
[13] For an interesting discussion of computer crimes, see T. Whiteside, *Computer Capers* (Thomas Y. Crowell Co., 1978).
[14] 756 F.2d 986 (4th Cir. 1985).
[15] *Id.* at 990.
[16] *Id.* at 990, 991.
[17] *See, e.g., United States* v. *Ortiz*, 422 U.S. 891 (1975). *See also Johnson* v. *United States*, 333 U.S. 10 (1948).
[18] 595 F.Supp. 171 (W.D.N.Y. 1984).
[19] *Id.* at 178.
[20] *Id.* at 177.
[21] *Id.*
[22] *United States* v. *Truglio*, 731 F.2d 1123 (4th Cir. 1984), cert. denied, 83 L. Ed.2d. 130 (1984).
[23] *Id.* at 1128.
[24] *Id.* at 1128.
[25] *Id.*
[26] *Sgro* v. *United States*, 287 U.S. 206 (1932).
[27] *Illinois* v. *Gates*, 462 U.S. 213, 238 (1983).
[28] *See* Fitzgerald and Eaton, *Fundamentals of Data Communication*, pp. 42–43 (John Wiley & Sons, 1978).
[29] *United States* v. *Harvey*, 540 F.2d 1345 (8th Cir. 1976).
[30] *Id.* at 1354.
[31] *United States* v. *McManus*, 719 F.2d 1395 (6th Cir. 1983).
[32] *Andresen* v. *Maryland*, 427 U.S. 463, 478 n. 9 (1976).
[33] U.S. Const. amend. IV.
[34] *See Marron* v. *United States*, 275 U.S. 192 (1927). For a thorough discussion, see 2 W. LaFave, *Search and Seizure* 95–101 (1978).
[35] *See* 2 W. LaFave, *Search and Seizure* 162 (1978).
[36] *Cf. Andresen* v. *Maryland*, 427 U.S. 463 (1976).
[37] *See, e.g., Steele* v. *United States*, 267 U.S. 498 (1925).
[38] *Supra* note 35, at 99.
[39] *Id.* at 104. *See, e.g., Quigg* v. *Estelle*, 492 F.2d 343 (9th Cir. 1974).
[40] 199 N.W.2d 514 (Minn. 1972).
[41] *Id.* at 515–516.
[42] *Supra* note 29, at 1353.
[43] *Id.* at 1354.
[44] *Id.*
[45] For a discussion of computer system components, see T. Schabeck, *Computer Crime Investigation Manual*, secs. 2.3–2.8 (Assets protection, 1980).
[46] An example of a detailed description of a computer system is: "One Alpha [Brand] Micro computer central processing unit, approximately four Alpha [Brand] Micro computer terminals, computer printers, and computer manuals, logs, printout files, operating instructions, including coded and handwritten notations, and computer storage materials, including magnetic tapes, magnetic discs, floppy discs, programs, and computer source documentation." Quoted from *Voss* v. *Bergsgaard*, 774 F.2d 402, 407 (1985) (warrant invalidated on other grounds).

Raiding the Computer Room
Fourth Amendment Considerations
(Conclusion)

"... the legal standard by which ... searches and seizures [of computers and computerized information] will be measured is the same as is applied to searches less concerned with modern technology."

By
JOHN GALES SAULS
Special Agent
FBI Academy
Legal Counsel Division
Federal Bureau of Investigation
Quantico, VA

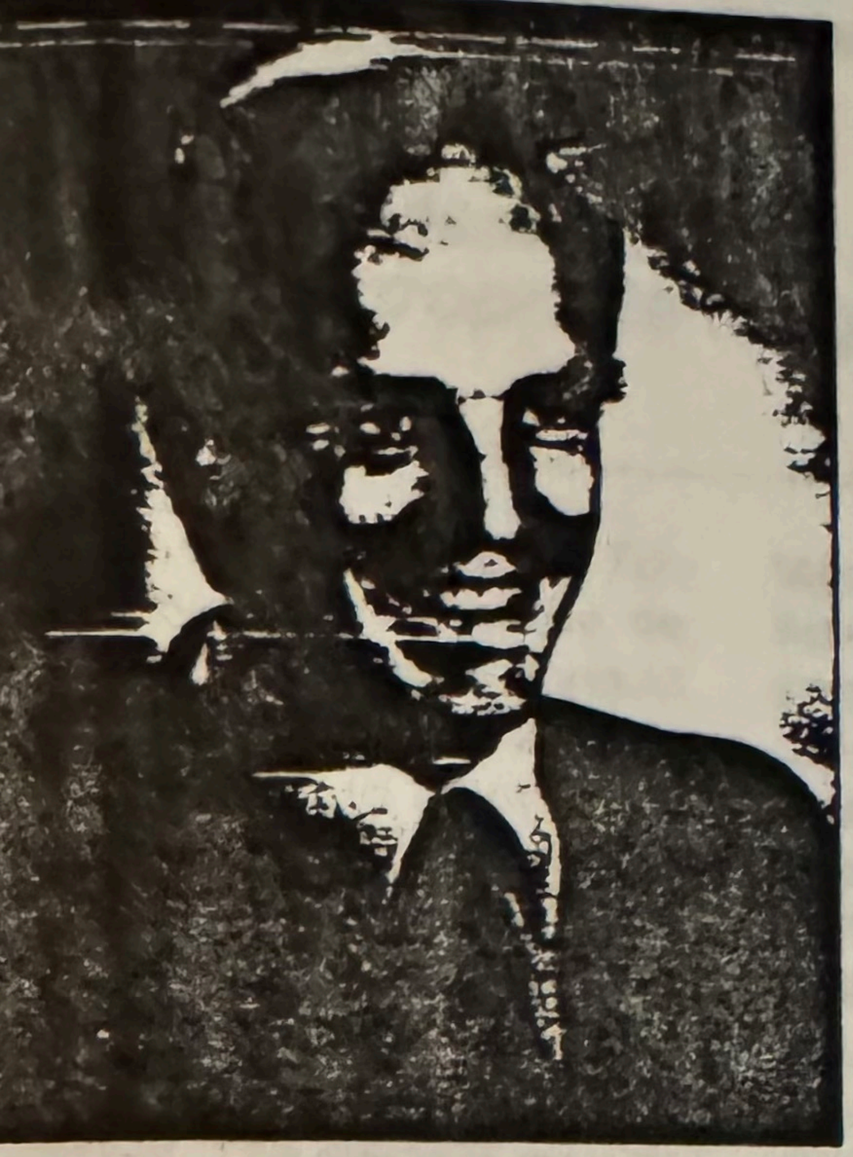
Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

Part I of this article examined the fourth amendment's requirements of establishing probable cause and particularly describing the items to be seized in affidavits which support warrants to search and seize computers and computer-processed information. Part I concluded with the particular description of computer equipment. Part II continues with a consideration of the particularity requirement as applied to computerized information and a discussion of fourth amendment standards regarding execution of search warrants on computer facilities.

Describing Computer-Processed Information

Officers seeking to describe particularly information that has been processed by a computer face two significant obstacles. The first obstacle is explaining in an affidavit for a search warrant that records being sought may be contained in sophisticated technological equipment. For example, digital computer systems store and process information in the form of electronic impulses.[47] For these purposes, this information is encoded into the binary number system, a "language" comprised only of the characters zero and one.[48] Since, for the officer seeking authority to search and seize and the court reviewing his application, "information (either numbers or text) in binary form is useless unless it can be decoded,"[49] describing computerized information in its encoded form is not meaningful. Fortunately, therefore, for officers drafting search warrant applications, this first obstacle is easily overcome, since officers are not required to confront the technological realities of what occurs when information is transformed into an electronic record. They can simply state that the information sought may be in electronic or written form.

It is the information itself that must be described with particularity, rather than the form in which the information may be found. Thus, if what is sought is "a letter from John Jones to Bill Smith dated November 9, 1985, and concerning the ownership of 200 shares of IBM stock," the letter should be described in those specific terms. The descriptive problem regarding whether the letter should be found in the form of paper with writing on it or magnetic tape electronically inscribed with binary code is solved by using more general terms. Concluding the description of the letter and similar items with the statement that "the records sought are 'written or electronic' " should be sufficient to permit lawful



Special Agent Sauls

seizures of the documents in either form, if the *information* sought is itself (as in the letter example) described with sufficient detail.[50] As previously noted, the storage media (magnetic discs, etc.) which could contain the information in electronic form should also be described as concisely as the facts known will allow.

The more-difficult obstacle then is particularly describing the information which is the object of the search. Information, whether recorded in written or electronic form, is generally collected into documents. Documents are what officers usually describe in warrants authorizing the seizure of information. Because the particularity requirement is strictly applied where documents are concerned,[51] the descriptive task is often a demanding one. Nonetheless, courts reviewing applications for search warrants evaluate the particularity of the description of a document in light of the degree of precision the facts of a case will allow.[52] The officer must be as precise as possible in describing a document, consistent with the facts that are available to him. The detailed description is required whether the information is computerized or not.

For example, in the *United States v. Timpani*,[53] a search warrant authorizing the seizure of "... any and all records relating to extortionate credit transactions (loansharking) ..."[54] was challenged as being insufficiently particular. In reviewing the warrant, the court noted that the warrant included a lengthy list of types of records (including "... lists of loan customers, loan accounts, telephone numbers, address books ..."[55]) and that the warrant "... provide[d] a standard for segregating the 'innocent' from the 'culpable' in the form of requiring a connection with [the] specific, identifiable crime [of loansharking]."[56] Approving the particularity of the warrant, the court stated, "... most important, it is difficult to see how the search warrant could have been made more precise."[57]

The task of the officer is to describe the information sought with sufficient particularity to avoid a forbidden "general" warrant. If he is aware of specific documents sought, he should designate them by type (letter, memo, etc.), date, subject, author, addressee, providing as much detail as possible. The earlier description of the letter regarding ownership of IBM stock is an example of this technique.

Where only the general nature of the information sought is known, a highly detailed description is impossible. In such cases, officers must use great care to give a description that includes the information sought but limits the search as narrowly as possible. This is accomplished by use of a general description that is qualified by some standard that will enable the executing officers to separate the information to be seized from innocent information that may also be present. This qualifying standard is known as a limiting phrase.

The limiting phrase must be crafted based on the facts establishing probable cause to search. If the facts establish that the information sought comes from a particular time period, the phrase should limit the warrant to information of that time period. If the information sought is known to have been produced by a particular individual, the phrase should limit the description to material authored by that person. If the phrase combines several such factors, it is even more ef-

"... it is often desirable to incorporate the affidavit into the warrant by appropriate language and to attach the affidavit to the warrant."

fective. As in *United States* v. *Timpani*, the phrase may restrict the description to particular criminal conduct. In that case, the limiting phrase was "... records relating to extortionate credit transactions (loansharking)...."[58] It is most important that the limiting phrase restrict the scope of the search so that it remains within the bounds of the probable cause set out in the affidavit. The warrant may not authorize the seizure of items for which probable cause to search has not been established. In upholding the description of items in the warrant in the *Timpani* case, the court noted that "[e]ach item is plausibly related to the crime—loansharking or gambling—that is specifically set out [in the affidavit]."[59] The description, even though the items to be seized were described in generic terms, did not exceed the probable cause because of the use of an appropriately narrow limiting phrase.

In *Application of Lafayette Academy, Inc.*,[60] a case involving a search for computerized information, the information sought was described in general terms with the inclusion of a limiting phrase, but the phrase was not made sufficiently narrow. Lafayette Academy, Inc., was being investigated for fraudulent activities in connection with their participation in the Federally Insured Student Loan Program (FISLP). The warrant authorized seizure of "books, papers, rosters of students, letters, correspondence, documents, memoranda, contracts, agreements, ledgers, worksheets, books of account, student files, file jackets and contents, computer tapes/discs, computer operation manuals, computer tape logs, computer tape layouts, computer tape printouts, Office of Education (HEW) documents and forms ... which constitute evidence of the commission of violations of the laws of the United States, that is violations of 18 U.S.C. Sections 286, 287, 371, 1001, and 1014...."[61] The probable cause in this case related to frauds pertaining to the FISLP. The court, in invalidating the search warrant, criticized the limiting phrase because it allowed seizure of items for crimes beyond the scope of the probable cause established. The court stated, "[t]he warrant is framed to allow seizure of most every sort of book or paper at the described premises, limited only by the qualification that the seized item by evidence of violations of 'the laws of the United States, that is violations of 18 U.S.C. Sections 286, 287, 371, 1001, and 1014.' The cited statutes, however, penalize a very wide range of frauds and conspiracies. They are not limited to frauds pertaining to FISLP, and there is no indication from the warrant that the violations of federal law as to which evidence is being sought stem only or indeed at all from Lafayette's participation in FISLP. Thus, the warrant purports to authorize not just a search and seizure of FISLP-related records as the government contends but a general rummaging for evidence of any type of federal conspiracy or fraud."[62] The court continued that "... the precise nature of the fraud and conspiracy offenses for evidence of which the search was authorized—fraud and conspiracy in the FISLP—needed to be stated in order to delimit the broad categories of documentary material and thus meet the particularity requirement...."[63]

Occasionally, the nature of the probable cause will allow a very broad description. In *United States* v. *Brien*,[64] a search warrant was issued for the premises of Lloyd, Carr & Company, a commodities brokerage firm. The warrant authorized the seizure of "Lloyd, Carr's bank statements, cash receipt books, option purchase records, sales material distributed to customers, employee compensation records, customer account records, sales training material and customer lists."[65] Noting that the described items constituted most of the business records of the company, the court nonetheless upheld the warrant's particularity, since the affidavit's facts "... warranted a strong belief that Lloyd, Carr's operation was, solely and entirely, a scheme to defraud...."[66] Since the facts in the affidavit established that *all* of the records of the business probably were evidence of the crime being investigated, the scope of the description was sufficiently particular. In upholding the validity of the warrant, the court stated, "... where there is probable cause to find that there exists a pervasive scheme to defraud, all the business records of an enterprise may be seized, if they are, as here, accurately described so that the executing officers have no need to exercise their own judgment as to what should be seized."[67]

The items to be seized should be described as precisely as the facts will allow, and items for which probable cause to search has not been established should not be included. An innovative means of limiting the items described to those for which probable cause to search has been established is found in the case *In Re Search Warrant Dated July 4, 1977, Etc.*[68] Here, the scope of the description of items to be seized was limited to documents related to "the crimes ... which facts recited in the accompanying affidavit

make out...."[69] The court, in upholding the warrant, noted with approval the limiting phrase. As was done in this case, it is often desirable to incorporate the affidavit into the warrant by appropriate language and to attach the affidavit to the warrant. Officers preparing search warrants for computerized information should consider the use of this procedure.

EXECUTING THE SEARCH WARRANT

The protection of the fourth amendment does not end when an officer obtains a valid search warrant. The right of citizens to be free of "unreasonable searches and seizures" extends to the manner in which a search warrant is executed.[70] For the search to be lawful, it must be done in a reasonable manner.[71] The U.S. Supreme Court has recognized the flexibility of this standard, stating "[t]here is no formula for the determination of reasonableness. Each case is to be decided on its own facts and circumstances."[72] Perhaps because of the vagueness of this standard, certain statutes also regulate the action of officers executing search warrants.[73]

Generally, officers must give notice of their authority and purpose prior to entering premises to execute a search warrant.[74] Once inside, the actions taken to secure control of the premises and prevent destruction of evidence must be reasonable under the circumstances.[75] The search itself must be performed within the scope of the warrant,[76] and care must be taken to cause no unnecessary damage during the search.[77] Finally, only items named in the search warrant may be seized, subject to a limited exception, the "plain view" doctrine.[78] These aspects of execution will be examined as they relate to computer searches.

The Announcement Requirement

To protect the privacy interests of citizens and the safety of both occupants of premises and the officers making entry to execute a warrant, officers are generally required to knock and announce their identity and purpose before forcibly entering premises to perform a search.[79] This requirement is subject to certain exceptions which allow entry without notice under some circumstances.[80] The exceptions include situations where the announcement would jeopardize the safety of the officers or others and where it would likely result in the destruction of evidence.[81] This latter exception, destruction of evidence, becomes relevant in searching for computer-processed information.

Due to the manner in which it is processed and stored, computerized information is easily and quickly destroyed. As previously discussed, information is encoded into the binary number system for processing purposes. This encoded information may then be stored in the computer's internal memory or on magnetic or other external storage media.[82] Generally, the internal memory is used to store data that must be immediately accessible to perform the tasks for which the computer is presently being used. Because any power interruption will result in the loss of information stored in the computer's internal memory, important information is usually duplicated and stored on an external storage device, such as a magnetic tape or disc. Information that is in the computer's internal memory that has not been "backed-up" by more permanent external storage may be destroyed in the instant it takes to flip a power interruption switch. Depending on the memory capacity of the computer, a considerable amount of information may be lost in this manner. Personal computers with internal storage capacities equal to 200 double-spaced typewritten pages are now common, and larger computers have much greater internal memory capacity. Information stored externally, especially if a magnetic storage medium is used, is likewise subject to rapid destruction. A device known as a degausser can instantly erase millions of data characters from a tape or disc.[83]

A pre-entry announcement is not required where officers know facts that cause them to reasonably believe that the making of an announcement will result in the destruction of evidence.[84] The ease and rapidity of destruction of the evidence sought is a factor courts will consider in determining whether a "no-knock" entry was reasonable.[85] Consequently, where officers know prior to execution of a warrant that information sought has been stored by computer and that persons with a motive to destroy the information are likely present at the place to be searched, an unannounced entry is likely reasonable.[86]

The announcement requirement is less stringently applied where warrants are executed against business premises.[87] Since computers are often located at businesses, this fact should also be considered in determining whether a pre-entry announcement is required.

Another alternative to the announced entry may exist when searching for processed data. Where computerized information is the target of the search, technology may allow the execution of the search without any physical entry. If the computer is one where access is available to persons with remote terminals via telephone lines, it is possible that the information sought

"Investigators executing a search warrant must use care to insure that the search is restricted to places where the items to be seized may be concealed."

may be obtained by an expert who "breaks in" the system remotely, using his own terminal and telephone.[88] Also, the electronic operations of some computer systems may be observed from as far away as one-half mile if the proper equipment is used.[89] Presumably, where no physical entry takes place, no announcement is required. Such searches do, however, fall within the application of the fourth amendment and its attendant requirements,[90] and in most cases, a search warrant will be required for performing such a search.[91] Additionally, some sort of notice to the operator of the computer that a search has been performed is likely required.[92]

Controlling The Premises

The U.S. Supreme Court has noted the utility of officers who are executing a search warrant exercising "unquestioned command of the situation."[93] Consequently, officers executing a search warrant have the power to control access to the premises being searched and to control the movements of persons present to facilitate the search and to prevent the removal or destruction of evidence. Due to the previously noted ease of destruction of computerized information and the size and complexity of some computer facilities, the need likely will exist to quickly take control of a computer facility being searched. Actions taken to control the premises and prevent the destruction of evidence will be evaluated based upon the reasonableness of the actions under the circumstances.

An example of this analysis is found in *United States* v. *Offices Known as 50 State Distrib.*,[94] where a search warrant was executed on a building housing a large "boiler room" sales operation that was engaged in fraud and misrepresentation in selling its promotional merchandise. About 50 local and Federal officers entered the premises to perform the search. At least 300 employees were present. The warrant authorized the seizure of almost all business records present. Upon entry, the officers required all persons present to remain at desks or in their assigned work areas. No one was permitted to go to the restroom without an escort. The court, in upholding the validity of the execution of the warrant, noted, "[t]he breadth of the warrant . . . rendered the execution of the warrant a most difficult task at best. Some control over the 300 . . . employees was necessary for an orderly search."[95]

Searching Within The Scope Of The Warrant

The requirement of a particular description of the items to be seized limits the allowable scope of a search in two ways. First, it restricts the places where an officer may look. An officer may look only in places where the item sought might reasonably be concealed.[96] Second, it restricts the time of execution. An officer may only search under the authority of the warrant until all named items have been located or seized or until all possible places of concealment have been explored.[97] Failure to comply with either of these restrictions can result in an illegal, general search that violates the fourth amendment.

Investigators executing a search warrant must use care to insure that the search is restricted to places where the items to be seized may be concealed. This can be quite difficult where records are sought and a great number of files are present. Regardless of the difficulty, reasonable steps must be taken to ensure that the search is no broader than authorized by the warrant.

A sensible first step is to make sure that all searching officers are aware of what items are listed in the warrant. In upholding the execution of the warrant in *In Re Search Warrant dated July 4, 1977 Etc.*, the court noted the procedure followed in that case, saying, "[i]n preparation for the search the agents attended several meetings to discuss and familiarize themselves with the areas and documents described in the search warrant and accompanying affidavit. They were instructed to confine themselves to these areas and documents in their search. During the search each agent carried with him a copy of the search warrant and its 'Description of Property' and could contact one of three persons on the scene who carried the supporting affidavit."[98] In upholding a warrant execution in *United States* v. *Slocum*,[99] the court also noted a pre-execution meeting.[100] Familiarizing the search team with the language of the warrant will increase the likelihood that a search will be performed in a manner a court will deem reasonable.

Once on the scene, the officers should continue to use care to restrict the search to the items listed in the warrant. A problem that frequently arises is that of sorting the items subject to seizure from those that are innocently possessed. This problem is especially common in cases where business records are the target of the search. In all cases, officers must restrict their search to places where the items named in the warrant are likely to be found and to limit the examination of innocent items to an extent no greater than that necessary to deter-

mine whether the item being examined is one of the items named in the warrant.[101] Again, the yardstick is reasonableness.

In many cases, a simple sorting process will be upheld as reasonable.[102] In *United States* v. *Slocum*, a warrant authorizing the seizure of business records related to illegal importation of tropical birds was executed. The U.S. Court of Appeals for the 11th Circuit described the execution process as follows: "... [T]he offices were a shambles and ... there was no apparent filing system; it was therefore concluded that it would be necessary to view each document to determine if it fell within the warrant. When an agent discovered a document that he or she believed covered by the warrant, the document was taken to one of four supervising agents who made the ultimate decision whether to seize the document."[103] The court approved use of "a common sense standard"[104] in evaluating the reasonableness of the search method and noted that where a warrant authorizes the seizure of documents, "some perusal, generally fairly brief, was necessary in order for police to perceive the relevance of the documents to the crime."[105] The court cautioned, however, that "the perusal must cease at the point of which the warrant's inapplicability to each document is clear."[106]

In Re Search Warrant Dated July 4, 1977, Etc. also concerned the execution of a search warrant requiring the examination of a multitude of documents. Fifteen agents conducted a search which lasted 9½ hours, during which they examined the contents of 93 file drawers, 14 desks, 3 bookshelves, and numerous boxes and piles of loose documents. The court described a systematic search where each document encountered was evaluated by search personnel to determine whether it fell within the description of items to be seized contained in the warrant. The U.S. Circuit Court of Appeals for the District of Columbia Circuit, in upholding the reasonableness of the search, noted that nothing in the record indicated a "general rummaging operation"[107] had taken place and that the agents involved in the search had been "... extensively briefed, instructed and supervised."[108]

Search for documents stored in electronic form by a computer will require use of the computer to view documents on a display screen or to print them by means of a printer. A sorting process similar to that employed in a search for "ink on paper" documents would seem reasonable under the circumstances. Such a sorting process was employed in *United States* v. *Harvey*.[109] There, an agent seeking, pursuant to a search warrant, an electronic device that produced telephone switching tones discovered some cassette audio tapes. He played about 12 of the tapes on a cassette player on the scene and determined that 2 contained recorded telephone switching tones. These tapes were seized. The U.S. Court of Appeals for the Eighth Circuit held these tapes were "properly seized as within the limitations of the warrant."[110] Use of computer equipment to examine computerized records should likewise be reasonable, since the records are otherwise incomprehensible to the searchers. Obviously, certain operational knowledge regarding the computer equipment will be required to perform this type of search. Under these circumstances, expert assistance during the search may be essential.[111]

The sorting process, performed at the scene of the search, serves to prevent the seizure, and thus the denial of access and use by the owner, of innocent records. The mere fact that the sorting process is time consuming will not make a wholesale seizure of records reasonable. Obviously, where a valid warrant authorizes the seizure of all business records, no sorting is required other than the elimination of nonbusiness records.[112] Otherwise, the reasonableness standard may require an arduous sorting process. Thus, where agents seized 11 cardboard boxes of computer printouts which were bound in 2000-page volumes, 34 file drawers of vouchers bound in 2000-page volumes, and 17 drawers of cancelled checks and hauled these records to another location where they sifted through them to extract the relevant documents (that were described in the search warrant) as a consequence of their determination that sorting at the site of the search would take a very long time, the seizure was held to be an unreasonable one.[113] Sorting at the scene of the search is generally required.

Certain characteristics of computerized recordkeeping may result in different treatment for computerized records.[114] First, the storage capacity of some computerized systems is such that review of all documents stored in the system could take a very long time. Second, unlike with paper files, the number of investigators who may assist in the search is limited by the number of computer terminals available for document display. Finally, where the records are stored magnetically, they may be quickly duplicated in their computerized form. Based on these considerations, it may be reasonable in some cases to duplicate the records quickly, leave copies for the use of the owner of the records, and seize the original records for later examination.

The likely legal concern in this situation is that the innocent documents included in the records would be available for unrestrained viewing by investigators resulting in a postponed "general search." A potential control for this problem would be continuing judicial supervision of the sorting process.[115]

Finally, when all items named in a warrant have been located and seized, the warrant provides no authority to continue the search.[116] Absent other legal justification, the search must terminate.

Avoiding Damage During a Search

A further requirement for the reasonable execution of a warrant is that the officers take care to avoid unnecessary damage to the property being searched and seized. Since computers are complex and fragile,[117] considerable care must be exercised where one is seized. Expert assistance may be necessary to ensure a damage-free seizure.

The "Plain View" Doctrine

As previously noted, an officer executing a search warrant will frequently need to sort through information to determine what portion of it may be seized pursuant to the warrant. If, during the course of the process, the allowed limited perusal of information is sufficient to cause the officer to conclude that the information is probable evidence of a crime, he is not required to leave the document behind, even though it is not described in the warrant. He may seize it under the "plain view" exception to the warrant requirement provided that he is lawfully present (searching reasonably within the scope of the warrant), it is readily apparent that the document is evidence, and the discovery of the document is "inadvertent" (that is, the officer did not possess probable cause to search for the document prior to beginning the search he is presently engaged in).[118]

CONCLUSION

Since judicial guidance is still limited in the area, investigators seeking and executing search warrants authorizing the seizure of computers and computerized information are on untested ground. However, the legal standard by which such searches and seizures will be measured is the same as is applied to searches less concerned with modern technology. Careful adherence to established fourth amendment principles, coupled with the use of expert assistance where needed, will enhance the likelihood of obtaining computerized evidence that is judicially admissible.

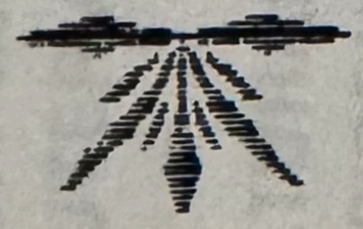
FBI

Footnotes

[47] 14 Am. Jur. *Proof of Facts 2d* 183 (1977).
[48] *Id. See also King v. State ex rel Murdock Acceptance Corporation*, 222 So.2d 393, 398 (1969).
[49] *Id.* at 184.
[50] *See United States v. Truglio*, 731 F.2d 1123 (4th Cir. 1984), *cert. denied*, 83 L.Ed.2d 130 (1984). *See also United States v. Offices Known as 50 State Distrib.*, 708 F.2d 1371 (9th Cir. 1983), *cert. denied*, 79 L.Ed.2d 677 (1984).
[51] *See Andresen v. Maryland*, 427 U.S. 463 (1976).
[52] For a thorough discussion, see Rissler, "Documentary Search Warrants," *FBI Law Enforcement Bulletin*, vol. 49, No. 7, July 1980, pp. 27–31.
[53] 665 F.2d 1 (1st Cir. 1981).
[54] *Id.* at 4.
[55] *Id.*
[56] *Id.* at 5.
[57] *Id.*
[58] *Id.* at 4.
[59] *Id.* at 5.
[60] 610 F.2d 1 (1st Cir. 1979).
[61] *Id.* at 3.
[62] *Id.*
[63] *Id.* at 3, 4.
[64] 617 F.2d 299 (1st Cir. 1980), *cert. denied*, 446 U.S. 919 (1980).
[65] *Id.* at 306.
[66] *Id.* at 308.
[67] *Id.* at 309, *contra Voss v. Bergsgaard*, 774 F.2d 402 (10th Cir. 1985).
[68] 667 F.2d 117 (D.C. Cir. 1981), *cert. denied*, 102 S.Ct. 1971 (1982).
[69] *Id.* at 141.
[70] *Go-Bart Importing Company v. United States*, 75 L.Ed. 374 (1931).
[71] *Id.*
[72] *Id.* at 382.
[73] An example is 18 U.S.C. §3109.
[74] *Cf. Ker v. California*, 374 U.S. 23 (1963) (concerning an entry to arrest). For a thorough discussion, see 2 W. LaFave, *Search and Seizure*, 122–140 (1978).
[75] *See United States v. Offices Known as 50 State Distrib.*, *supra* note 50.
[76] *Cf. Harris v. United States*, 331 U.S. 145 (1947). For a thorough discussion, see 2 W. LaFave, *Search and Seizure* 160–163 (1978).
[77] See 2 W. LaFave, *Search and Seizure* 161 (1978).
[78] *See Coolidge v. New Hampshire*, 403 U.S. 443 (1971). For a thorough discussion, see 2 W. LaFave, *Search and Seizure* 183–184 (1978).
[79] *Supra* note 74.
[80] *Id.*
[81] *Id.*
[82] See generally 16 Am Jur, Proof of Facts 265–291 (1965).
[83] D. Parker, *Fighting Computer Crime*, page 42 (Charles Scribner's Sons, 1983).
[84] *Supra* note 74.
[85] *Id.*
[86] *Id.*
[87] *See United States v. Francis*, 646 F.2d 251, 258 (6th Cir. 1981), *cert. denied*, 70 L.Ed.2d 616 (1981).
[88] For a discussion of the ease with which an expert can gain access to a supposedly secure system, see T. Whiteside, *Computer Capers*, pp. 117–121 (1978).
[89] T. Schabeck, *Computer Crime Investigation Manual*, section 9.2.9 (Assets Protection, 1980).
[90] *See Katz v. United States*, 389 U.S. 347 (1967).
[91] *Id.*
[92] *See Berger v. New York*, 388 U.S. 41 (1967).
[93] *Michigan v. Summers*, 452 U.S. 692, 703 (1981), citing 2 W. LaFave, *Search and Seizure* 150–151 (1978).
[94] *See United States v. Offices Known as 50 State Distrib.*, *supra* note 50.
[95] *Id.* at 1376.
[96] *Supra* note 76.
[97] *Id.*
[98] *Supra* note 68, at 123.
[99] 708 F.2d 587 (11th Cir. 1983).
[100] *Id.* at 601.
[101] See generally 2 W. LaFave, *Search and Seizure* 173–178 (1978).
[102] *See, e.g., In Re Search Warrant Dated July 4, 1977, Etc.*, *supra* note 68. *See also United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982).
[103] 708 F.2d 587, 602 (11th Cir. 1983).
[104] *Id.* at 604.
[105] *Id.*
[106] *Id.*
[107] *Supra* note 68, at 124.
[108] *Id.*
[109] *United States v. Harvey*, 540 F.2d 1345 (8th Cir. 1976).
[110] *Id.* at 1354.
[111] An expert accompanied officers executing the search warrant in *Ottensmeyer v. Chesapeake & Potomac Telephone Co.*, 756 F.2d 986 (4th Cir. 1985). Another case considering the role of an expert accompanying officers executing a search warrant is *Forro Precision, Inc. v. International Business Machines Corp.*, 673 F.2d 1045 (9th Cir. 1982).
[112] *See United States v. Brien*, *supra* note 64.
[113] *United States v. Tamura*, *supra* note 102.
[114] *See e.g., United States v. Tamura*, *supra* note 102.
[115] *Id. See also DeMassa v. Nunez*, 747 F.2d 1283 (9th Cir. 1984) (special master appointed to supervise sorting of documents during search of attorney's office).
[116] In addition to suppression of evidence, civil liability may result when a search continues after all items named in warrant have been seized. *See Creamer v. Porter*, 754 F.2d 1311 (5th Cir. 1985).
[117] For a discussion of the ways a computer may be physically damaged, see *Fighting Computer Crime*, *supra* note 82, pages 41–42.
[118] *Supra* note 78.

INVESTIGATIVE TECHNIQUES

A PRACTICAL GUIDE



Wayne Cerow

Cerow Investigations
and Consultants

INVESTIGATION

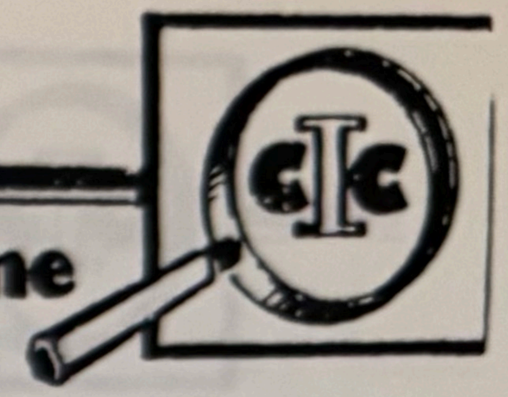
Computer Crime Investigation

INITIAL INTERVIEW

- COLLECT INFORMATION TO DETERMINE IF THE COMPUTER ABUSE WAS:
  - NATURAL CAUSED
  - ACCIDENTIAL
  - INTENTIONAL

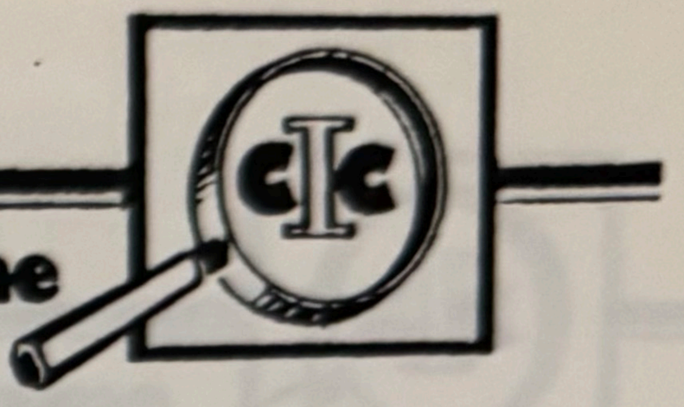
- COLLECT INFORMATION TO DEVISE AN INVESTIGATION PLAN.

INVESTIGATION
INITIAL INTERVIEW — LISTEN



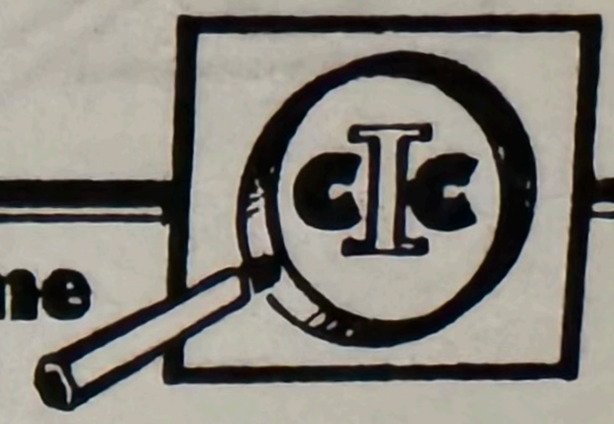
- TAKE EXTENSIVE NOTES, PREFERABLY RECORD THE INTERVIEWS.
- ALLOW THE VICTIM / REPRESENTATIVE TO RELATE ALL FACTS BEFORE QUESTIONING.
- INTERVIEW WHERE THERE WILL BE NO INTERRUPTIONS.
- RELATE THE FACTS BACK TO THE VICTIM/ REPRESENTATIVE, CLARIFYING ALL TERMINOLOGY.

INITIAL INTERVIEW — ASK



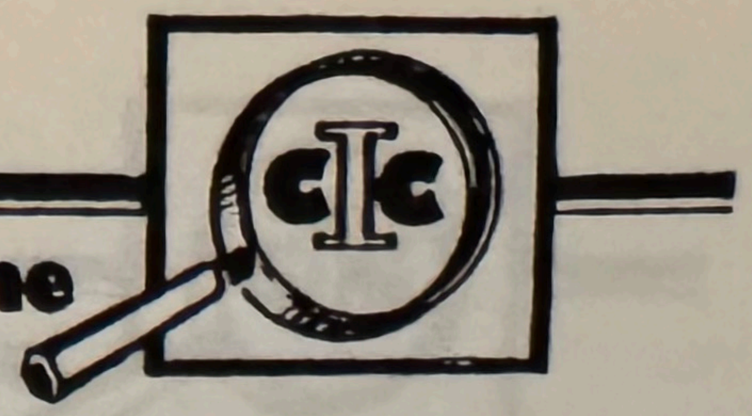
- WHY HE BELIEVES A COMPUTER ABUSE WAS COMMITTED (IF NOT APPARENT)
- HOW HE BELIEVES IT WAS COMMITTED
- WHAT SAFEGUARDS WERE COMPROMISED
- WHERE THE COMPROMISE COULD OCCUR
- WHO COULD HAVE COMMITTED THE ABUSE
- WHO WOULD BENEFIT FROM THE ABUSE
- WHAT WAS THE OBJECT OF THE ABUSE
- WHO MAY ALSO HAVE INFORMATION RELEVANT TO THE INVESTIGATION

INFORMATION



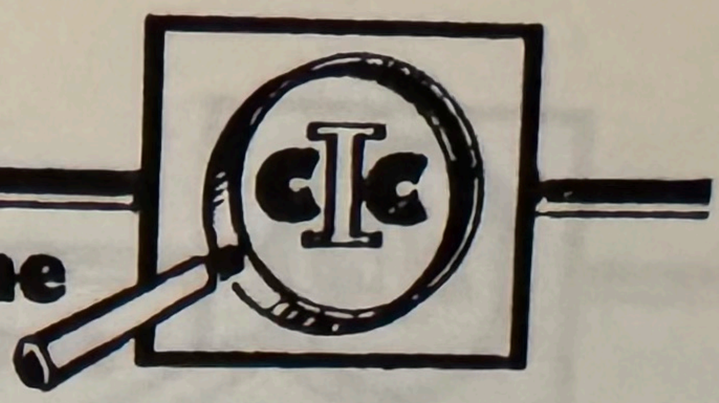
- COMPUTER SYSTEM
- SECURITY MEASURES
- AUDITING MEASURES
- CORPORATE STRUCTURE
- PERSONNEL INFORMATION

INFORMATION COMPUTER SYSTEM



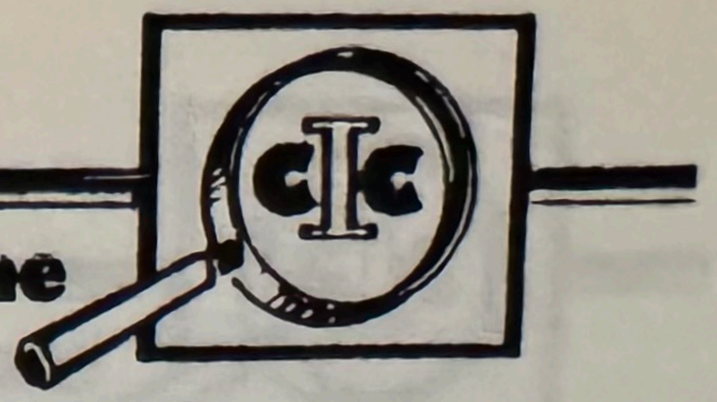
- SYSTEM APPLICATION
- INTERNAL USERS
- OUTSIDE USERS
- SYSTEM DATA FLOW
- INPUT DATA PREPARATION
- OUTPUT DATA DISTRIBUTION
- SYSTEM CONFIGURATION
  - NUMBER OF DIAL-UP LINES
  - NUMBER OF PRIVATE LINES
  - LOCATION OF TERMINALS
  - LOCATION OF TELEPHONE JUNCTION BOXES

INFORMATION SECURITY MEASURES



- PHYSICAL SECURITY
  - COMPUTER CENTER
  - BACK-UP CENTER
  - SUPPLIES
  - TERMINALS
- LOGICAL SECURITY
  - TERMINAL ACCESS
  - FILE ACCESS

INFORMATION AUDITING MEASURES



- INTERNAL AUDITING
  - PROCEDURES
  - AREA OF RESPONSIBILITY
  - RESULTS OF LAST AUDIT
- EDP AUDIT
  - PROCEDURES
  - AREA OF RESPONSIBILITY
  - RESULTS OF LAST AUDIT

INFORMATION
CORPORATE STRUCTURE

Computer Crime Investigation

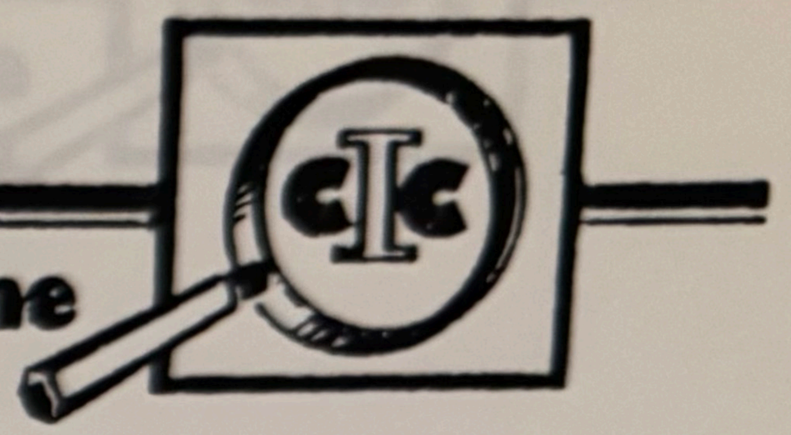
- REPORTING STRUCTURE
- JOB DESCRIPTION
- AREA OF RESPONSIBILITY

INFORMATION PERSONNEL

Computer Crime Investigation

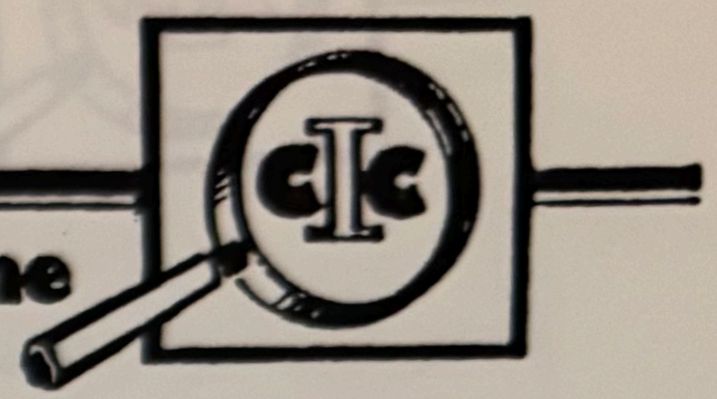
- **NEW HIRES**
- **RESIGNATIONS**
- **TERMINATIONS**

CORPORATE RESOURCES



- CORPORATE SECURITY
- CORPORATE AUDITING
- SYSTEM PROGRAMMERS
- COMPUTER CENTER PERSONNEL
- PERSONNEL DEPARTMENT
- COMPUTER SUPPLIER
- CORPORATE LAWYER

INVESTIGATION PLAN



- DOCUMENTED
- CONFIDENTIAL
- SPECIFY A TEAM LEADER
- DEFINE INDIVIDUAL RESPONSIBILITIES
- UTILIZE INFORMATION AND RESOURCES FROM THE INITIAL INTERVIEW
- THOROUGH, BUT FLEXIBLE

CHARTING METHODS

Computer Crime
Investigation

- FLOW CHARTS
- COINCIDENCE CHARTS
- TIME LAPSE CHARTS

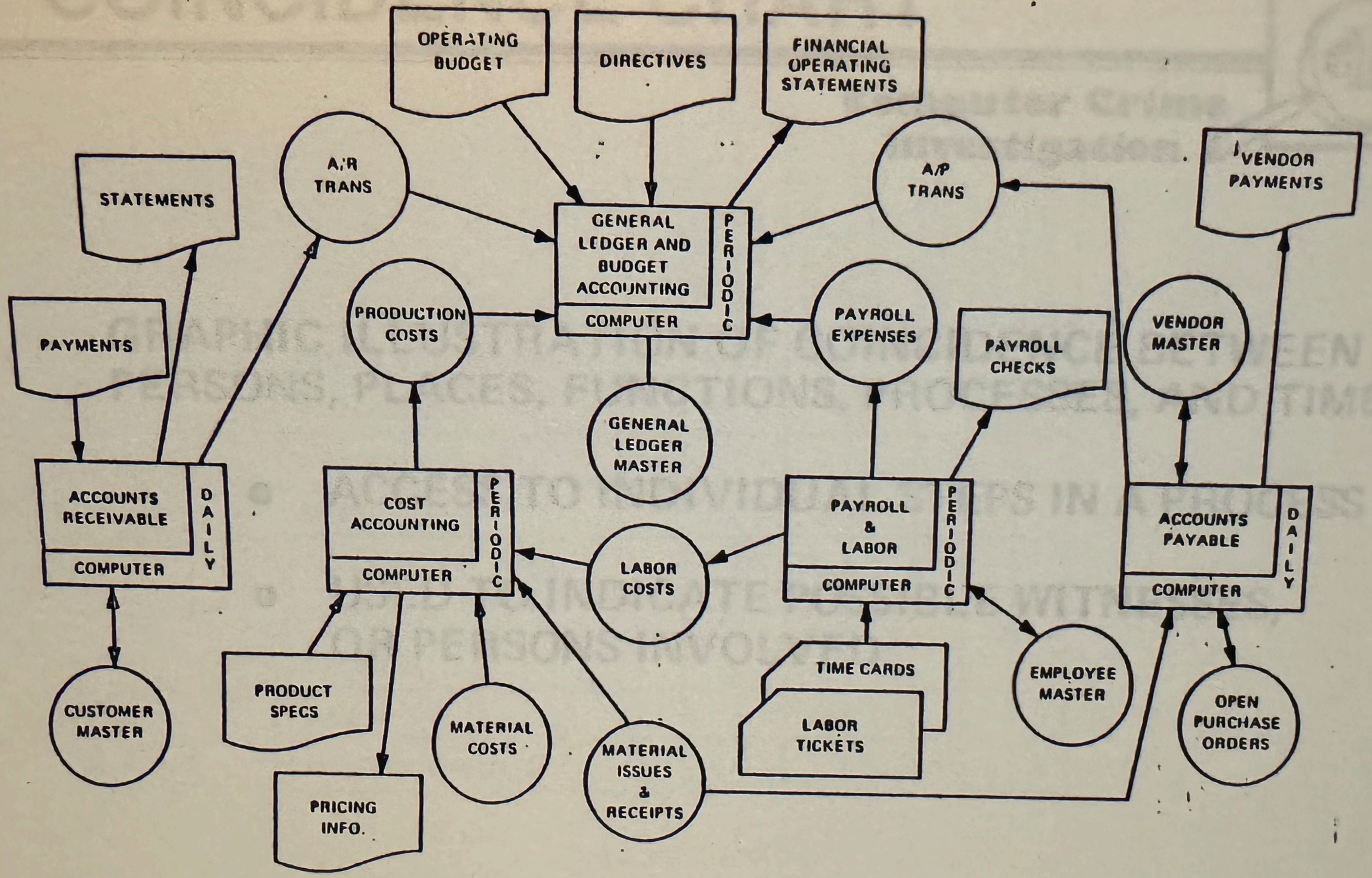
FLOW CHART

Computer Crime Investigation

CAN BE USED AS AN AID IN UNDERSTANDING COMPLEX INFORMATION

- SOFTWARE PROGRAMS
- PROCESS/FUNCTION FLOW
- INDIVIDUAL MOVEMENTS
- ILLUSTRATION OF INVESTIGATION PLAN

FINANCIAL CONTROL – DESIGN PROTOTYPE



COINCIDENCE CHART

Computer Crime Investigation

GRAPHIC ILLUSTRATION OF COINCIDENCE BETWEEN PERSONS, PLACES, FUNCTIONS, PROCESSES, AND TIME

- ACCESS TO INDIVIDUAL STEPS IN A PROCESS
- USED TO INDICATE POSSIBLE WITNESSES, OR PERSONS INVOLVED

COINCIDENCE CHART

Computer Crime Investigation

	SECRETARY	FORMAN	KEYPUNCH CLERK	SUPERVISOR	OPERATOR A	OPERATOR B	INPUT CLERK
ACCESS TO TIME CARD	X	X	X	X			
DISTRIBUTES	X	X					
COLLECTS		X					
SIGNS		X					
ACCESS TO KEY PUNCH	X	X	X	X			
KEY PUNCH			X	X			
DELIVERS				X			
PICK UP				X			
COMPUTER INPUT					X	X	X

ASSOCIATION MATRIX

TIME LAPSE CHART

Computer Crime Investigation

WED. USED EMP. TAPE

MON. 10 AM

TUES 2 AM

WED TAPE BAD

PAYROLL

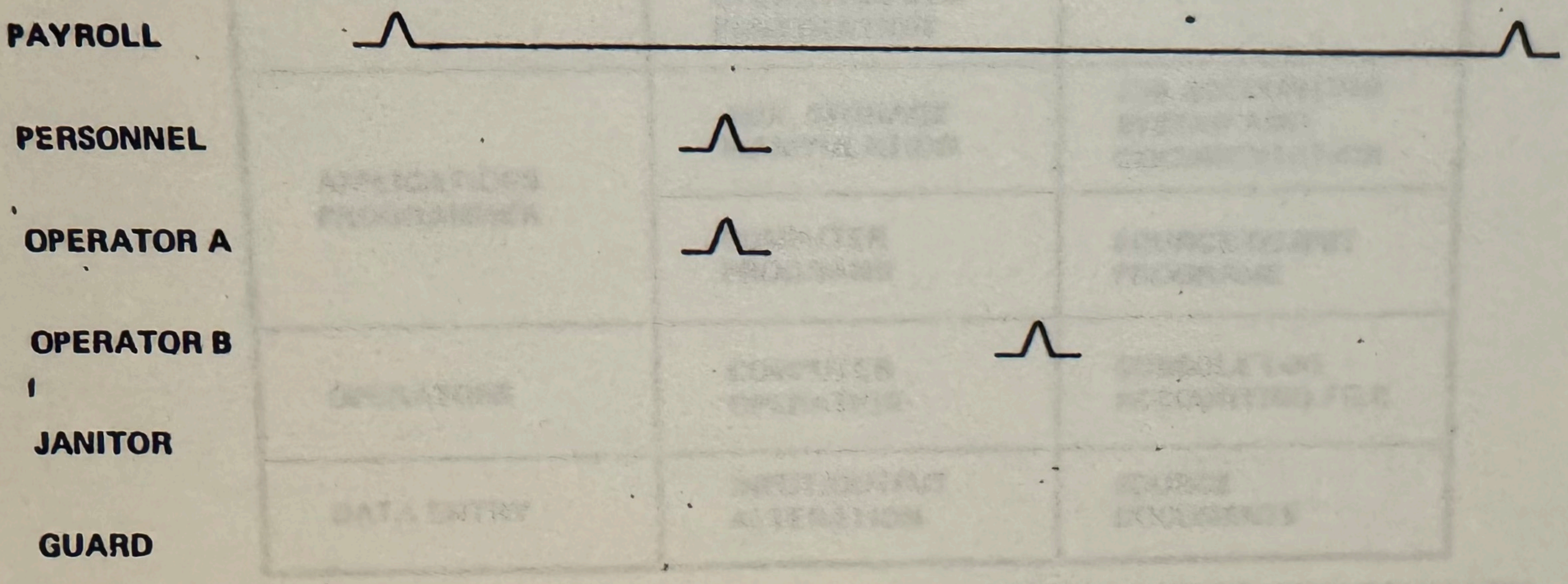
PERSONNEL

OPERATOR A

OPERATOR B

JANITOR

GUARD



SCHEMES & CAPABILITIES CHART

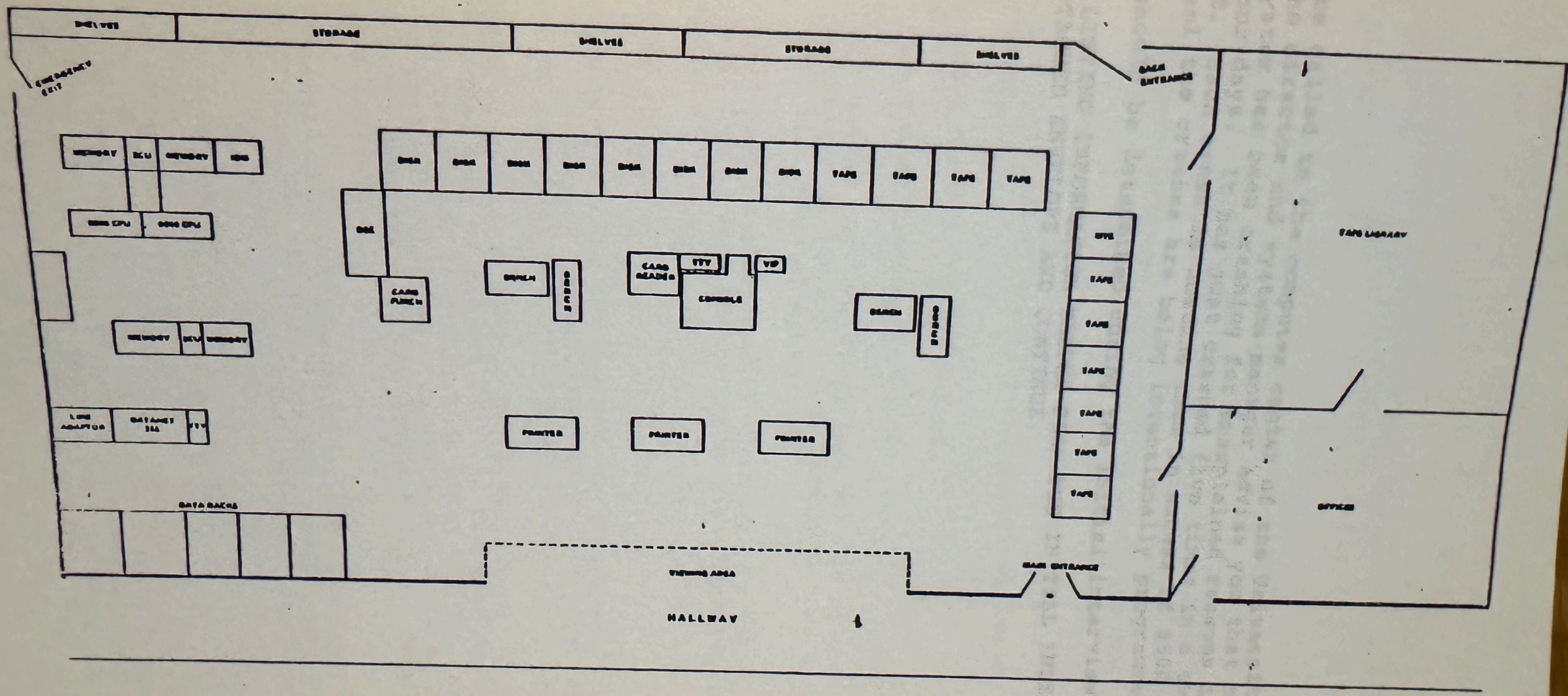
Computer Crime Investigation

PERSONNEL CAPABILITIES	SCHEMES	SOURCE OF EVIDENCE
SYSTEM ANALYST AND PROGRAMMER	COMMUNICATIONS	COMMUNICATION LOG AND DOCUMENTATION
	OPERATING SYS. PENETRATION	
APPLICATIONS PROGRAMMER	AUX. STORAGE MANIPULATION	JOB ACCOUNTING SYSTEM AND DOCUMENTATION
	COMPUTER PROGRAMS	SOURCE/OBJECT PROGRAMS
OPERATORS	COMPUTER OPERATION	CONSOLE LOG ACCOUNTING FILE
DATA ENTRY	INPUT/OUTPUT ALTERATION	SOURCE DOCUMENTS

FBI LAW ENFORCEMENT BULLETIN
JULY, 1979

FIGURE 2

COMPUTER CENTER LAYOUT



CASE NO. 1

You are called to the computer center of the University Campus. The director and systems manager advise you that the computer system has been crashing for unexplained reasons in the last four days. It has just crashed five times in a two hour period. Each crash is costing them in excess of $500 and they feel the crashes are being intentionally programmed.

What should be determined during the initial interview?

AFTER LISTING INFORMATION NEEDED FROM THE INITIAL INTERVIEW, OPEN THE ATTACHED ENVELOPE AND CONTINUE.

The following information should have been determined during the initial interview.

SYSTEM CONFIGURATION:

1. The XYZ system is housed in a central location on campus and has more than 75 employees.

2. The computer performs tasks ranging from storage of student admission files to advanced theoretical physics calculations.

3. 120 remote terminals are utilized from on-campus and off-campus locations.

4. Direct connect and dial lines are both utilized.

   - Direct lines allow immediate and unlimited use of the computer.

   - Two phone numbers for dial lines.

     - One number provides unlimited use.

     - One number provides 10-minutes service only with an automatic disconnect. Dial line uses a 40 line rotary into the computer system.

5. User ID code must be entered when connecting to the system. This is used for billing and to prevent unauthorized use of the computer.

SYSTEMS MANAGERS STATED:

1. Person(s) responsible for the crashes was making small technical errors while modifying the program, which allowed systems personnel to interpret the program and identify two individuals.

   One individual was identified by his system ID of "ABCD" which preceeded many of the crashes. He has been employed by the computer center on a part time basis but was terminated because of personal conflicts. He was later employed full time by a different department in the computer field. He works in the physics building.

   The second individual was identified by the file "AA01" where the crash program was stored. This was accomplished by the system trace after the crash. This individual was a student employed part time by the computer center assigned to a remote location in the basement of the library. A printout of the file was made. The program was decoded and the only use was to crash the system. Subject "AA01" called for his file and ordered a set of punch cards containing the crash program to be sent to the basement of the library. Subject "AA01" had been caught removing and using unauthorized systems information two months before the crashes started, but was disciplined and allowed to continue employment.

From the information gathered in the initial interview.

1. What is your plan to apprehend the suspect/s?

2. What information will be regarded as evidence?

3. Present the facts to the class as if they were the jury of lay persons who do not know computers.

4. What security measures were compromised, if any?

5. What security measures would have prevented the abuse?

6. List any auditing procedures that would help in the detection or investigation of the abuse.

CASE STUDY:

You are a police investigator assigned to the organized crime unit of your department.

You are called to the city managers office where the city manager and the city auditor inform you of the following circumstances. The auditors ran a new program against the accounts payable file to check for duplicate payments. The program indicated that three authorized invoices were each paid twice.

The city manager stated that a federal auditor is coming in four weeks and you are being called in on the initial investigation.

What team members will you need for your investigation?

What is your investigation plan?

What elements must you prove to prosecute in Arizona?

What evidence will you gather?

CASE NO. 2

Officer Jones served a search warrant on the home of Mr. Joe Smith as a result of an undercover fencing operation that was conducted by the Podunk Police Department. Mr. Joe Smith had sold to the fencing operation a number of negotiable securities that were taken in burglaries throughout the city.

While executing the search warrant, officers found pages of computer printout with the names, addresses, and securities owned by the individuals listed.

Further investigation revealed that some of the people listed on the computer printout were victims of the burglaries. After interviewing the victims, it was determined that they all used the brokerage services of the Greater Securities brokerage firm.

Officer Jones interviewed Mr. Smith and was told that he (Mr. Smith) acquired the list of names from a middle man for $1,000 and he does not know the middle man or the person who gave the list to him.

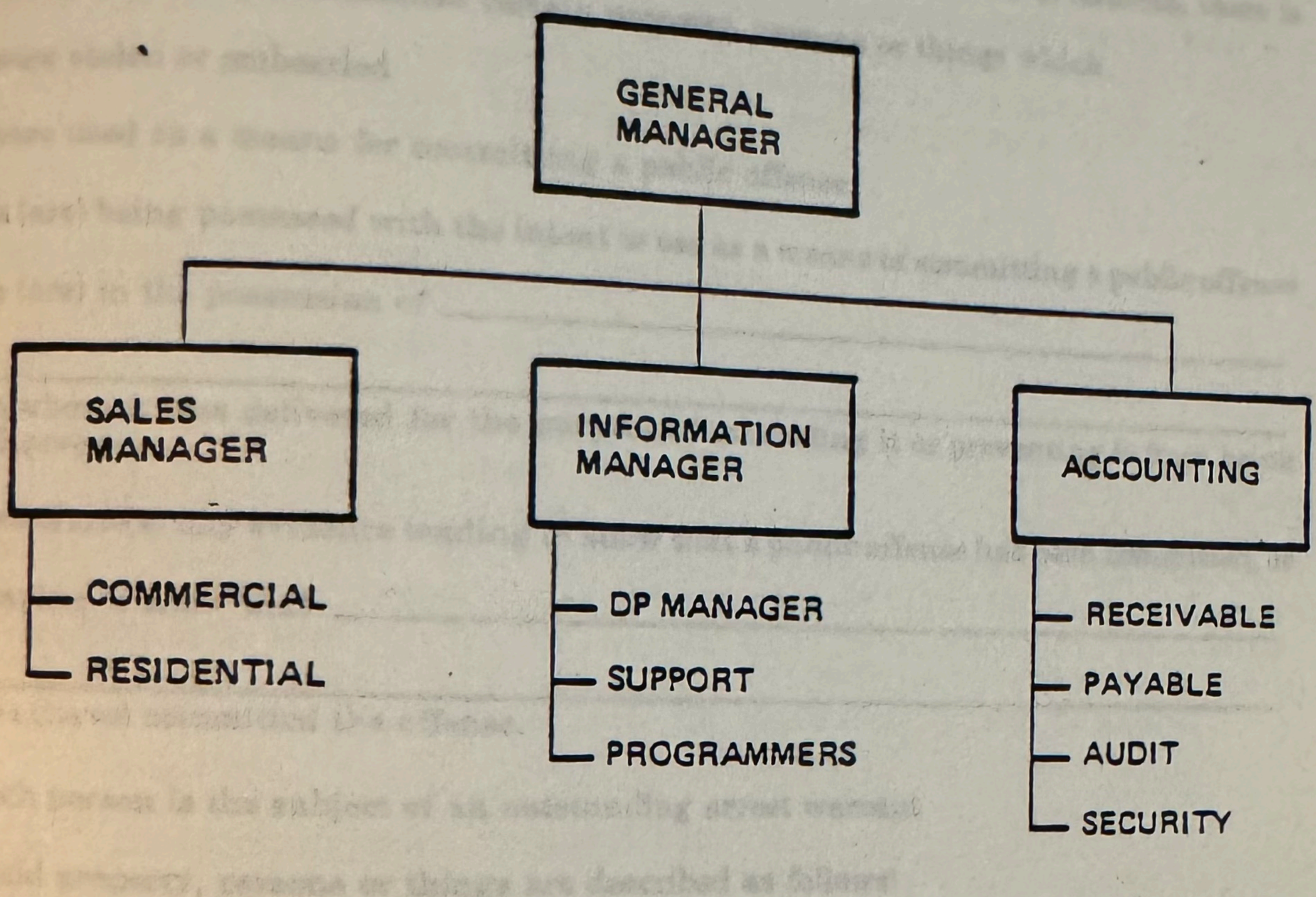
Officer Jones contacted Mr. James, general manager of the Greater Securities brokerage firm and advised him of the information that he had acquired and asked him if he would cooperate in determining how Mr. Smith came in possession of the computer printout with the list of clients.

Will Mr. James cooperate with Officer Jones?

If Mr. James cooperates, how should the investigation proceed?

List:

A) ASSUMPTIONS
B) SAFEGUARDS
C) POSSIBLE AREAS OF COMPROMISE
D) EVIDENCE GATHERED TO SUPPORT YOUR FINDINGS


GENERAL MANAGER
SALES MANAGER
INFORMATION MANAGER
ACCOUNTING
COMMERCIAL
RESIDENTIAL
DP MANAGER
SUPPORT
PROGRAMMERS
RECEIVABLE
PAYABLE
AUDIT
SECURITY

in the City of Phoenix , County of Maricopa , State of Arizona, there is now being possessed or concealed certain property, persons or things which

( ) were stolen or embezzled

(X) were used as a means for committing a public offense

(X) is (are) being possessed with the intent to use as a means of committing a public offense

( ) is (are) in the possession of _____

_____

to whom it was delivered for the purpose of concealing it or preventing it from being discovered

( ) constitute(s) any evidence tending to show that a public offense has been committed, or

tending to show that _____

_____

has (have) committed the offense.

( ) such person is the subject of an outstanding arrest warrant

That said property, persons or things are described as follows:

Unknown make/model computer (possibly a portable, personal computer) including a console input cevice, a printer output device, printer listings, a modem device, magnetic disks, magnetic diskettes (floppy disks), cassette tapes, magnetic tapes, computer instruction/operating manuals, computer programs (software) and instruction manuals, tapes, books, records, ledgers, correspondence memoranda, computer flow charts, block diagrams and other documentation which show computer program descriptions, computer logs and historical data. Any documentation listing the phone numbers (602) 275- , (713) 227- , (602) 951- , (602) 951- , any 6-digit numbers, and the company names " " or " Inc.".

EVIDENCE CONSIDERATIONS IN DATA PROCESSING INVESTIGATIONS

U.S. Constitution

Article (IV)

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Federal Rules Of Criminal Procedures

Rule 41. Search and Seizure

Property or Persons Which May Be Seized With a Warrant. A warrant may be issued under this rule to search for and seize any (1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense; or (4) person for whose arrest there is probable cause, or who is unlawfully restrained.

Rule 16. Discovery and Inspection

(a) Disclosure of Evidence by the Government.

(1) Information Subject to Disclosure

. . .

(c) Documents and Tangible Objects - Upon request of the defendant the government shall permit the defendant to inspect and copy or photograph books, papers, documents, photographs, tangible objects, buildings or places, or copies or portions thereof, which are within the possession, custody or control of the government, and which are material to the preparation of his defense or are intended for use by the government as evidence in chief at the trial, or were obtained from or belong to the defendant.

FEDERAL RULES OF EVIDENCE

Hearsay

Rule 801. Definitions

The following definitions apply under this article:

(a) Statement.--A "statement" is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by him as an assertion.

(b) Declarant.--A "declarant" is a person who makes a statement.

(c) Hearsay.--"Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.

Rule 802. Hearsay Rule

Hearsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress.

Rule 803. Hearsay Exceptions; Availability of Declarant Immaterial

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

. . .

(6) Records of regularly conducted activity.--A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

admissible

(7) Absence of entry in records kept in accordance with the provisions of paragraph (1).--Evidence that a matter is not included in the memoranda reports, records, or data compilation, in any form, kept in accordance with the provisions of paragraph (1), to prove the nonoccurrence or nonexistence of the matter, if the matter was of a kind of which a memorandum, report, record, or data compilation was regularly made and preserved, unless the sources of information or other circumstances indicate lack of trustworthiness.

(8) Public records and reports.--Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.

(10) Absence of public record or entry.--To prove the absence of a record, report, statement, or data compilation, in any form, or the nonoccurrence or nonexistence of a matter of which a record, report, statement, or data compilation, in any form, was regularly made and preserved by a public office or agency, evidence in the form of a certification in accordance with rule 902, or testimony, that diligent search failed to disclose the record, report, statement, or data compilation, or entry.

Authentication and Identification

Rule 901. Requirement of Authentication or Identification

(a) General Provision.--The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

(b) Illustrations.--By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

(1) Testimony of witness with knowledge.--Testimony that a matter is what it is claimed to be.

. . .

(7) Public records or reports.--Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public

record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

. . .

(9) Process or system.--Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

Rule 902. Self-Authentication

Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

. . .

(4) Certified copies of public records.--A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1),(2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

Contents of Writings, Recordings, and Photographs

Rule 1001. Definitions

For purposes of this article the following definitions are applicable:

(1) Writings and recordings.--"Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostatic, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

(2) Photographs.--"Photographs" include still photographs, X-ray films, video tapes, and motion pictures.

(3) Original.--An "original" of a writing or recording is the writing or recording itself of any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

(4) Duplicate.--A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or

by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

Rule 1002. Requirement of Original

To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.

Rule 1003. Admissibility of Duplicates

A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

Rule 1005. Public Records

The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, <u>including data compilations in any form</u>, if otherwise admissible, may be proved by copy, certified as correct in accordance with rule 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given.

Rule 1006. Summaries

The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.

<u>Expert Witnesses</u>

Rule 702. Testimony by Experts

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise.

Rule 703. Bases of Opinion Testimony by Experts

The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to him at or before the hearing. If of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject, the facts or data need not be admissible in evidence.

INVESTIGATIVE TECHNIQUE: MAIL COVERS

A "mail cover" is the process by which a record is made of any data appearing on the outside cover of any class of mail, including checking the contents of any second-, third-, or fourth-class mail as now sanctioned by law, in order to obtain evidence of a crime.

The U. S. Postal Service maintains supervision with respect to the use of mail covers as investigative techniques. Postal Inspectors in Charge may order mail covers within their districts where a written request is received from any Federal, state, or local government specifying the reasonable grounds that exist which demonstrate that the mail cover would assist in obtaining information concerning a crime. Where time is of the essence the Inspector in Charge may act upon an oral request to be confirmed in writing within two business days. However, no information will be released until an appropriate written order is received.

Mail cover orders do not remain in effect for more than 30 days, but additional 30 day requests may be authorized. A mail cover may not remain in effect for more than 120 days without the personal approval of the Chief Postal Inspector. No mail cover report may include matter mailed between the mail cover subject and his/her attorney. Mail covers should not remain in force after the subject has been indicted, except when the purpose of the mail cover is to obtain information on further criminal violations or to assist in the location of a fugitive.

Any inquiries or problems concerning mail covers should be directed to the Fraud Section at FTS 724-7127. More specific information is also available in Title 39, Code of Federal Regulations, Section 233.3 et seq. (1984) and the United States Attorneys' Manual, 9-4.200 et seq.

ELECTRONIC MAIL AND DATA TRANSMISSION

James R. Hastings
Special Attorney
Organized Crime and
Racketeering Section
Office (FTS) 633-3707

Thomas A. Blair
Assistant United States Attorney
Southern District of Florida
Office (FTS) 350-5201

Electronic (non-voice) communications play an essential role in the American business community. Not surprisingly, some of the most sophisticated forms of electronic communications are also being used by organized criminal networks, especially in connection with clandestine financial transactions.

"Electronic mail" has been defined as a method of moving and storing information and messages electronically. An "electronic mailbox" is any sort of computer or data terminal which can send and receive electronic mail. In 1978 there were only 5,000 "electronic mailboxes" in use in the United States. By the end of 1981 that number had increased to 80,000.

While teletype continues to be the most reliable form of non-voice wire communication in many parts of the world (especially Central and South America), the advent of widespread electronic mail has made teletype technologically obsolete for use in the United States. The advantages of electronic mail over traditional telegraphic communication include speed, portability, ease of remote access, the ability to store records at remote locations, the transmission of data over regular telephone lines, and the ability to transfer funds electronically (electronic banking).

Electronic mail services in the United States are quite numerous and include Ontyme II, GE Information Systems, The Source, STWC, Compuserve, CCA, Telemail, Dialcom, Easylink Instant Mail (ESL), MCI Mail and Delphi. Of these services, two (Compuserve and The Source) merit detailed attention because of their great popularity as general information networks available to the public. Two others (Easylink and MCI Mail) merit attention because of their direct access to the international telex network.

Both Compuserve and The Source provide an inexpensive subscription service through which any subscriber may communicate with any other subscriber by home computer or data terminal over ordinary telephone lines. Each service assigns its subscribers an account number and an individual password. The user may then call the service's mainframe computer, enter his account number and password, and then leave message for other subscribers or retrieve messages which have been left for him. Transmissions over telephone lines to and from the host computer are generally at 300 characters per second (300 baud), but may be as fast as 1200 baud, or as slow as 110 baud.

Once a user has read the messages in his electronic mailbox, he may either file (store) the messages for later use or erase them immediately.

Of course, since the host computers of any electronic mail system will respond to any data transmission so long as the user identifies himself by account number and password, users with portable terminals or TDD's (telephone devices for the deaf) may call in from any telephone in North America.

Public Data Networks, such as Tymnet, Uninet, and Telenet can be used to access most electronic mail facilities within the United States from many foreign countries, using either 300 or 1200 baud transmission. Datapac is the major Public Data Network in Canada. International rate information and sign-on instructions are available from the data networks. These public data networks are frequently referred to as Value Added Networks (VANS) or Packet Switched Networks.

Some of the individual features of the above-mentioned systems are explained below:

Compuserve

Compuserve is a subsidiary of H & R Block Company and is located at 5000 Arlington Centre Boulevard, P. O. Box 20212, Columbus, Ohio 43220. Compuserve subscriptions are marketed through Radio Shack (a major supplier of home computers). There is no monthly fee, and the night-time user rate is very reasonable. Subscribers in major American cities may access the system through local telephone numbers, thereby leaving no traceable long distance telephone bill. Users outside metropolitan areas may access the system through the Public Data Networks Telenet and Tymnet for a small additional fee. Canadian users may use DATAPAC (another value added common carrier) for an additional hourly charge. Naturally, a connection made via one of the common carriers creates a traceable long distance telephone bill, but only from the user's telephone to the carrier's nearest access number.

Example #1: A money launderer living in Northern Virginia could communicate with a courier in Philadelphia by calling Compuserve's Washington, D.C., access number (202) 352-7506. The courier would call (215) 563-0814 in Philadelphia. Both of them could communicate with their superior in Miami, who would call (305) 667-3564. None of these communications would involve a long distance call.

Example #2: A money launderer in San Francisco could communicate with a courier in Lincoln, Nebraska by calling the San Francisco access number (415) 956-4191, which is a local call. The nearest direct access number which the courier in Lincoln could use would be (402) 895-7131 in Omaha, but this would be a toll call. Instead, the courier can call the local Tymnet number in Lincoln. The fee for this service is $2.00 per hour, but eliminates the traceable toll call.

Example #3: A cocaine importer travelling in the United States could communicate with his partner in Fort Pierce, Florida from any major city without leaving a toll record. The Fort Pierce partner can either (1) call Compuserve's direct access number in Fort Lauderdale, or (2) call closer Tymnet numbers in Melbourne or West Palm Beach. In any event, a toll record is generated, but in the case of a call to Tymnet, there will be no way to show that the call ultimately went to Compuserve.

In addition to its electronic mail service, Compuserve provides a variety of other services. Of particular interest are the banking and brokerage services. Compuserve subscribers may transfer funds electronically among four banks and one money market fund, i.e., Shawmut Bank of Boston, Huntington National Bank (Columbus, OH), Central Trade Bank of Memphis, First Tennessee Bank (Knoxville, TN) and Liquid Green Trust (a money market fund).

The Source

The Source is operated by Source Telecomputing Corporation, a subsidiary of Reader's Digest, 1616 Anderson Road, McLean, Virginia 22102.

The Source has a small minimum monthly charge. Users in the Washington, D.C., area may call directly on The Source's local numbers. Outside the Washington metropolitan area, access is through the common carriers Telenet and Uninet. Canadian calls are made through DATAPAC. As an alternative, subscribers may use The Source's WATS number. There is a small per-minute surcharge for the use of the 800 number, but note that the surcharge is added to the user's Source bill, not his telephone bill since calls to 800 numbers are not charged to the caller.

The Source may be accessed on Telenet from more than fifty foreign countries including the Bahamas, Colombia, Peru, Switzerland and the Virgin Islands.

Unlike Compuserve, The Source does not provide any electronic banking services. However, in addition to electronic mail, The Source does lease its subscribers virtually unlimited electronic storage space for documents and records. Use of this storage feature can be identified upon examination of a user's monthly billing statements.

It is this record storage facility which makes The Source particularly attractive to the criminal element. The records of any criminal enterprise in North America may be safely stored "off site" and accessed from any telephone.

MCI Mail and Easylink Instant Mail (ESL)

Most major teletype carriers in the United States are now operating their own electronic mail services. The two most popular systems are Easylink Instant Mail (ESL), operated by the Western Union Telegraph Company, and MCI Mail. These systems not only receive and forward electronic mail, but, of even greater importance to the criminal investigator, they also offer direct access to the worldwide telex network. Thus, from anywhere in the United States, a money launderer could dial 800-325-4050, 800-325-4112 (ESL) or 800-323-0905 (MCI Mail) and use either of these electronic mail systems to send or receive a telex message to or from Colombia, Panama, etc., without creating a telephone toll record of any kind. Both MCI Mail and Easylink have local access numbers in most metropolitan areas throughout the United States in addition to the 800 number indicated above.

Encryption Systems

Although no case has arisen involving encrypted electronic mail or electronic files, publicly available computer systems and devices exist which could seriously hamper the interception of electronic data for law enforcement purposes.

Two such proprietary devices are CX-II and Hermes-4, both manufactured by Cryptext Corporation of Seattle, Washington. Both of these are hardware encryption devices specifically designed to be driven by common microcomputers. The CX-II costs less than $1000, and the current price for the Hermes-4 is under $500. The Cryptext system provides security which exceeds the National Bureau of Standards' data encryption standard.

Experts Study Effect on Law Of Latest Electronic Services

By DAVID BURNHAM
Special to The New York Times

WASHINGTON, March 17 — A few months ago, Leo Radosta of Detroit pleaded guilty to involvement in a cocaine trafficking ring and was sentenced to 10 years in Federal prison.

For at least two years, Mr. Radosta and 12 of his associates were the subject of a special kind of investigation that raised, but in the end did not answer, a series of complex new questions about the kinds of legal protections that should be extended to information in the computer age.

The questions were raised when a Federal grand jury requested the Source Telecommunications Company, a subsidiary of Reader's Digest, to provide it with "any and all records, writing or documents, including printouts of any and all records, data, documents or electronic mail" about Mr. Radosta, his associates and their companies.

The lack of Federal laws to protect the tens of millions of electronic messages now being transmitted each year by Source Telecommunications and a growing number of other companies offering similar services was the focus of a conference here recently.

The Ethical Use of Computers

The conference was organized by Jerry Berman, an attorney for the American Civil Liberties Union, and by the Public Interest Computer Association to examine the impact of new technologies on the law.

The conference was unusual in that it brought together staff members from a half-dozen Senate and House subcommittees involved in communications law; officials from a number of major corporations, including the American Telephone and Telegraph Company, the International Business Machines Corporation and GTE Telenet, as well as Source Telecommunications, and such leading privacy experts as John Shattuck, a vice president of Harvard Univerasity, Allen F. Westin, professor of public law and government at Columbia University, and Ronald Plesser, a Washington lawyer and former general counsel of the now defunct Privacy Protection Study Commission.

The conference was not limited to examining the efforts of law-enforcement agencies to penetrate computerized data bases. Of at least equal concern was the lack of Federal laws to handle individual and corporate snoopers.

Source Telecommunications is a relatively new kind of company that offers more than 37,000 subcribers various electronic information and communication services through its computers and telephone network.

An Electronic Filing Cabinet

One of the services it offers, for example, is a kind of electronic filing cabinet in which a subscriber who has his own personal password may privately store, change or delete information. Other services allow subscribers to exchange electronic messages.

But when attorneys for Source Telecommunications and its customers argued that the electronic messages held by the company were mechanically but not legally under its control, Leonard R. Gilman, the United States Attorney in Detroit, contended in a responding brief that the material requested by the grand jury was not protected by law or judicial rulings that guard a telephone call or letter from examination without a warrant.

The consensus at the conference appeared to be that technology had outgrown existing Federal law and that Congress ought to close the loopholes.

A spokesman for the United States Attorney's office in Detroit said Source Telecommunications provided the grand jury with billing information about the targets. But legal questions about information the company held that belonged to its customers were not resolved, the spokesman said, because the targets were indicted before a judicial decision was handed down.

Electronic mail companies are subject to other kinds of searches, the nature of which makes estimating their actual threat difficult to measure.

In the last few years there have been a number of highly publicized cases in which young computer experts or disgruntled employees or former employees have broken into the computers of private corporations or government agencies.

There are indications, however, that this type of penetration by individuals may be only one aspect of the problem.

Five months ago, for example, Walter G. Deeley, the senior intelligence official responsible for protecting sensitive Government information, charged for the first time publicly that electronic surveillance by the Soviet Union, foreign intelligence agencies and a number of major corporations posed a threat to national security.

And most major oil companies are reported to be so concerned about corporate espionage that they regularly encode seismographical and drilling data transmitted electronically.

A '$100 Million Industry'

Electronic mail companies represented a "$100 million industry," Michael F. Cavanagh, executive director of the Electronic Mail Association, a trade group that represents about 40 major companies, told the conference. He predicted that by the early 1990's the companies would gross at least $1 billion a year.

The participants decided that devising solutions for the industry's legal problems would require both the passage of new laws and amendments to existing laws.

Generally, they appeared to agree on two goals. The first was the passage of laws establishing standards when law-enforcement agencies could appropriately obtain warrants to get information held by electronic mail companies.

The second was adoption of a narrowly worded Federal statute to be used in the prosecution of corporate spies and others who rifled the computer data bases of private companies.

SAMPLE SUBPOENA (NUMBER SEVEN) TO OBTAIN BILLING RECORDS AND SUBSCRIBER INFORMATION FOR EASYLINK INSTANT BAIL (WUT. CO.)

SUBPOENA TO TESTIFY BEFORE GRAND JURY

United States District Court	DISTRICT: Northern District of Virginia
TO: WESTERN UNION TELEGRAPH COMPANY NATIONAL EASYLINK BILLING & COLLECTION CENTER ONE MARKET STREET SAN FRANCISCO, CA	SUBPOENA FOR: ☐ Person ☒ Document or Object

YOU ARE HEREBY COMMANDED to appear in the United States District Court at the location, date and time specified below to testify before the Grand Jury in the above entitled case

PLACE	COURTROOM
Federal Building 701 Prince Street Alexandria, Virginia	Room Number 777
	DATE AND TIME 7:07 a.m. July 7, 1987

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):

A. Copies of all "summary of charges," "notices," "summary of departments," "statement of charges," "summary of services," "Easylink Services," "detail of other charges/credits," invoices, billings, and all related documents for the prior six month period; and

B. All subscriber "sign-up" forms, subscriber requests and related documents identifying or associated with any Easylink ID Number, Easylink User Name, Easylink Mailbox Address Number, Easylink Telex Number, CI Telex Answerback, Western Union Billing Account Number, and all Mailbox User Names;

Identifiable with any of the following names, organizations, or identification numbers:

1. EASYLINK ID: EID476100
2. EASYLINK USER NAME: INTLVEG
3. EASYLINK MAILBOX ADDRESS: 62690602
4. EASYLINK TELEX: 353228
5. ANSWERBACK: JR HASTINGS

☒ Please see additional information on reverse

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court.

CLERK	DATE
Jane J. Jones, Clerk, U. S. District Court	7/7/87
BY, DEPUTY CLERK /s/ Sam S. Smith, Deputy Clerk	

This subpoena is issued on application of the United States of America by:

SAMPLE SUBPOENA

NAME, ADDRESS AND PHONE NUMBER OF ASSISTANT U.S. ATTORNEY

James R. Hastings
Post Office Box 7258
Ben Franklin Station
Washington, D. C. 20044-7258
Phone (202) 633-3707
633-3708

EASYLINK INSTANT MAIL

THE ELECTRONIC MAIL SERVICE OF
WESTERN UNION TELEGRAPH COMPANY

Local Access Numbers for 16 major metropolitan areas are listed in alphabetic order. If you are located in one of these cities, simply select the phone number which corresponds to your Baud Rate.

There are no special instructions for dialing up these numbers.

	Access No.
Atlanta	
110	404/659-3637
300	404/659-3583
1200	404/659-3606
Boston	
110	617/482-8693
300	617/482-8744
1200	617/482-8715
Chicago	
110	312/263-2314
300	312/263-3723
1200	312/263-2347
Cincinnati	
110	513/241-2488
300	513/241-2819
1200	513/241-2901
Dallas	
110	214/939-0450
300	214/939-0452
1200	214/939-0454
Detroit	
110	313/962-4390
300	313/962-4417
1200	313/962-4393
Houston	
110	713/237-0361
300	713/237-0431
1200	713/237-1254
Kansas City	
110	816/221-3888
300	816/698-0008
1200	816/698-0015

	Access No.
Los Angeles	
110	213/624-3213
300	213/624-3227
1200	213/624-4248
Miami	
110	305/371-4081
300	305/371-6382
1200	305/371-6385
New Orleans	
110	504/524-9845
300	504/524-9744
1200	504/524-9645
New York	
110	212/608-7313
300	212/608-7332
1200	212/608-7480
Philadelphia	
110	215/592-4379
300	215/592-4496
1200	215/592-4377
San Francisco	
110	415/989-6310
300	415/989-6383
1200	415/989-6300
St. Louis	
110	314/241-5440
300	314/241-5601
1200	314/241-6141
Washington D.C.	
110	202/638-7694
300	202/638-7679
1200	202/638-7669

* Customer Service: (800) 424-6677
* In Washington, call: (202) 833-8484

Following are MCI Mail local access phone numbers:

Atlanta, GA	(404)	577-7363
Baltimore, MD	(301)	583-6850
Boston, MA	(617)	262-6468
Buffalo, NY	(716)	847-6050
Chicago, IL	(312)	856-9000
Cincinnati, OH	(513)	651-1204
Clearwater, FL	(813)	586-0955
Cleveland, OH	(216)	771-7177
Columbus, OH	(614)	221-3451
Dallas, TX	(214)	754-0461
Denver, CO	(303)	831-8139
Detroit, MI	(313)	962-5980
Ft. Worth, TX	(817)	338-4159
Hackensack, NJ	(201)	488-2622
Hartford, CT	(203)	728-1909
Honolulu, HI	(808)	545-3050
Houston, TX	(713)	850-1005
Indianapolis, IN	(317)	634-2208
Jacksonville, FL	(904)	358-1749
Kansas City, MO	(816)	474-3169
Largo, FL	(813)	586-0955
Long Island (Garden City Area), NY -	(516)	596-0404
Los Angeles, CA	(213)	620-1449
Memphis, TN	(901)	523-9314
Miami, FL	(305)	381-9012
Milwaukee, WI	(414)	347-1769
Minneapolis, MN	(612)	893-9462
Naperville, IL	(312)	369-0805
Newark, NJ	(201)	623-0295
New York City, NY	(212)	245-0355
Oakbrook, IL	(312)	850-9511
Oakland, CA	(415)	540-1114
Philadelphia, Pa	(215)	636-9060
Phoenix, AZ	(602)	266-1148
Pittsburgh, PA	(412)	261-9918
Rochester, NY	(716)	955-9850
Sacramento, CA	(916)	442-6986
San Diego, CA	(619)	268-1708
San Francisco, CA	(415)	543-1560
San Jose, CA	(408)	995-6711
Santa Ana, CA	(714)	550-7128
Seattle, WA	(206)	282-3077
Sherman Oaks, CA	(818)	906-8989
Stamford, CT	(203)	325-8133
St. Louis, MO	(314)	991-1881
St. Petersburg, FL	(813)	586-0955
Tampa, FL	(813)	221-1597
Washington, DC	(703)	525-6500
White Plains, NY	(914)	232-7527

- National Toll-Free Access Number -

----------(800) 323-0905----------

Recording Data Communications

Recently drug violators have cooperated with investigators by using their telephone and home computer terminal to access drug related information located in another city. It is highly desirable to document these consensual "data conversations" for the same reasons that voice communications of cooperative individuals are tape recorded and maintained as evidence. Since this is a relatively new area, a few general suggestions are offered to assist investigators first faced with this situation.

1. Just as with the consensual recording of voice conversations, it is always necessary to obtain a written and witnessed waiver of rights from every cooperating individual. Applicable agency regulations should also be followed.

2. The tape recorder that is now being used for the recording of voice conversations may also be very adequate for the recording of data communications. A cassette recorder such as the Radio Shack Model CCR-81 (Cat. No. 26-1208) or equivalent model seems to work well and is relatively inexpensive. Cassette recorders designed for loading data into home computers do not utilize the same frequencies that are employed with data communications transmitted over telephone lines. Some systems are relatively close while others are not. So, just because a recorder is designed to pick up data from a home computer does not necessarily mean that it will also perform well when recording data transmitted over the telephone.

3. One easy method of using the tape recorder to intercept a "data conversation" is with the use of a Telephone Recording Control, such as the Radio Shack Catalog No. 43-228 or equivalent model. The Recording Control uses modular connectors and is placed between the telephone instrument used for placing the call and the telephone wall jack. Follow the hookup instructions supplied with the unit. [This recording control unit will also function if placed between the terminal modem and the telephone wall jack should that become necessary.]

4. The control unit has two small plugs attached for interfacing with the tape recorder. The smallest plug, which is normally placed into the monitor jack of the tape recorder should be left unused for this application. The

tape recorder is turned on manually prior to placing or receiving a telephone call. The larger plug is placed into the microphone imput jack of the tape recorder. Check to be sure that connections are firm and that the tape recorder is using AC power and not batteries.

No attempt should be made to playback the recording through the equipment of the cooperating individual. Playback should be attempted only with the assistance of a trained technician.

Two "channels" will have been recorded on the tape at the same time. The cooperating individual has transmitted data over the "low frequency band," and received data from the "high frequency band." A printout made of the "high band" by playing the tape through a modem set in the "originate" position will produce only the data that the cooperating individual received at that end of the conversation. Likewise, a printout made of the "low band" by playing the same tape through a modem set in the "answer" position will produce only that data which was transmitted by the cooperating individual. This would probably include identification numbers and passwords. Therefore, all printouts made from recorded data conversations should be identified by clearly marking with either "originate modem" or "answer modem" to indicate whether the printout is a copy of the data contained on the high or low band of that particular conversation.

This recording technique will allow the investigator to document most electronic mail, "home phone" teletype, alphanumeric pager transmissions and home computer terminal communications.

Further information can be obtained from James R. Hastings, Special Attorney, Organized Crime and Racketeering Section, Criminal Division, FTS 633-3707, and Thomas A. Blair, Assistant United States Attorney, Southern District of Florida, FTS 350-4833.

COHERENT COMMUNICATIONS SYSTEMS CORP

60 Commerce Drive, Hauppauge, New York 11788
Telephone: 516-231-1550
New York: 212-895-6316
Telex 96-1439

FSR-89A DUAL F1/F2 (BELL 103) MONITOR

GENERAL

The FSR-89A is a stand-alone, asynchronous receive-only, dual demodulator designed for monitoring low speed Telex or data traffic on a two-wire voice frequency facility. A typical application for the FSR-89A is to obtain immediate copy of traffic at a location not close to the data terminal.

The FSR-89A bridges accross the VF line and permits monitoring data transmitted from either end of the circuit. In addition, a composite signal combining the traffic from both ends of the circuit is provided for use with terminals operating half-duplex.

The unit, which is Bell 103 compatible, converts frequency shift signals to digital signals suitable for direct connection to EIA RS-232-C or CCITT V.28 interfaces. A four-wire version is available upon request.

SPECIFICATIONS:

Compatibility:	Bell 103 compatible.
Maximum Data Rate:	0 to 300 BPS.
Operating Mode:	Half or Full Duplex.
Operating Range:	0 to -45dBm.
Input Impedance:	High impedance (bridging) or, 600 ohms 2-wire balanced.

Receive Frequencies (Hz):

	ORIG	ANS
Mark	2225	1270
Space	2025	1070

Power Requirements:	16VAC (47-63Hz) 375mA AC adapter supplied for either 115VAC or 220VAC operation.
Physical Dimensions:	Height: 2.44 in. (6.22 cm.). Width: 8.50 in. (21.60 cm.). Depth: 9.25 in. (23.50 cm.).
Weight:	FSR-89A: 32 ounces (912 gm.). AC adapter: 8.1 ounces (230 gm.).

HANDOUT

Lesson: Planning the Investigation

Investigative Team Members

1. EDP Auditor - Highly skilled auditor who specializes in computer related activities. May be familiar with several different computer systems. Generally has in-depth knowledge of one type of system, can write computer programs and possibly utility programs in at least one advanced language, and can use various utility programs and pre-packaged audit software.

2. EDP Investigator - (very hard to find) Experienced in investigating computer related activities. May be able to write basic programs and run utility programs. Knows what available pre-packaged software can do and how to use the results. Is familiar with available documentation and data processing personnel roles.

3. Case/project manager - May have limited experience with computers, but has extensive investigative experience in complex cases.

4. Criminal Investigator - Has general knowledge of computer terminology and awareness of vulnerable areas in computer systems. Is aware of fraud indicators or flags and understands basic investigative concerns such as evidence, elements of proof, interviewing, constitutional rights, etc. Can communicate with data processing personnel and can trace the flow of data through a computer system.

5. Prosecutor - Has prosecuted complex cases including cases involving computer related activities or evidence.

6. Computer Systems Analyst - Has extensive knowledge of the computer system involved in case. May have been included at design stage. Understands the entire operation of the specific computer system. Usually can write programs in at least one advanced language.

7. Security Specialist - Has skills in identifying vulnerable areas in computer system. May or may not have a data processing background. Generally controls system access through assignment of passwords and security codes. Has control over security programs if any exist on system.

8. Programmer - Skilled in at least one advanced language. May write systems programs, communications programs, applications programs or any combination.

9. Data Clerk - Converts data from source documents to computer media when given appropriate entry instructions.

10. Computer Operator - Has overall knowledge of operation of computer system hardware for at least one system. May have programming skills.

11. Technical/Electronic/Communications Specialist - May or may not be an investigator with specialized knowledge of electronic or communications equipment useful to the investigation.

12. Vendor Customer Engineer - Has detailed knowledge of specific computer equipment and/or vendor supplied software. May or may not have been involved in initial installation of equipment at computer site.

INVESTIGATIVE WORKPLAN

SE TITLE Green, Harvey

SE NUMBER - 123-45-83

VESTIGATOR - Jones

NAGER - Smith

Investigative Leads	Date	Results
Received Complaint Workplan	10-25-83	
1. Interview Complainant.		
2. Check Internal Security files. Delete Suspects Password		
3. Check IRS files.		
4. Contact Computer Branch Security Specialist.		
5. Contact Internal Audit for computer expertise.		
6. Check TECS for police records.		
7. Possibly interview other employees in section.		
8. Research federal and state statutes.		
9. Contact AUSA/identify elements of crime to be proven.		
10. Confront/interview subject if needed.		

INVESTIGATIVE WORKPLAN

CASE TITLE Green

CASE NUMBER - 123-45-83

INVESTIGATOR - Jones

MANAGER - Smith

Investigative Leads	Date	Results
	10/30/83	Computer Security Specialist advised Green has possibly misused computer system. Printout looks like some kind of stocks/bonds program with capability to do market analysis.
Amended Plan		
11. Secure Green's files/data from being erased or destroyed.		
12. Obtain copy of Green's program/data **EVIDENCE**.		
13. Determine how often program was run and cost to gov't.		
14. Determine if Green is using other unauthorized programs/ data.		
15. Discuss Green's level of access to system with Computer Branch Chief to determine if Green's access should be limited to prevent further misuse/fraud.		
16. Possible surveillance of Green.		
17. Track Green's current computer activity if level of access is not restricted.		
18. Seek expert advise re: similar cases if available.		

January 1985
Volume 4
Number 1

COMPUTER MATCHING

A Message from the HHS Inspector General

By Richard P. Kusserow

We are pleased to welcome The Council of State Governments (CSG) as the new publisher of our **Computer Matching** newsletter. The newsletter has become an invaluable outlet for sharing information about computer matching and other automated screening and verification techniques. As a state-supported and state-directed organization, CSG serves to strengthen federal/state relationships. It is now in an excellent position to act as a conduit for this vital information exchange.

Without question, computer matching and automated verification have taken on a new emphasis with the passage of the Deficit Reduction Act (PL 98-369). The income and eligibility verification section of the act is a direct outgrowth of the President's Council on Integrity and Efficiency's Long Term Computer Matching Project. Some of the key provisions, such as using the Social Security number for matching purposes and standardizing formats, had long been advocated by the project.

We are working with the interagency task force responsible for drafting regulations to implement the provisions of the Deficit Reduction Act. The notice of proposed rulemaking for the AFDC, Medicaid, food stamp and unemployment insurance programs will be published for comment in the near future.

We urge all states to review these regulations carefully and to submit comments about any needed changes or clarifications. The perspective of state governments is crucial to the successful implementation of these important provisions.

Eight states in Southeast match food stamp rolls

To determine how many food stamp recipients are collecting benefits in more than one state, eight southeastern states have used computer matching. The Southeast Interstate Match Project, involving Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee, is the largest cooperative undertaking by states to measure and analyze duplicate food stamp participation.

All eight state food stamp agencies provided their Food Stamp Program eligibility lists for November 1983 to the Florida Division of Public Assistance Fraud, the agency that coordinated the initial phase of the review and conducted all the computer work. Florida matched the Social Security numbers and other available identifiers, such as the names and

(Continued on page 2)

This newsletter is published by The Council of State Governments for the Long Term Computer Matching Project of the President's Council on Integrity and Efficiency. The Project Co-Chairmen are Richard P. Kusserow, Inspector General of the U.S. Department of Health and Human Services, and J. Brian Hyland, Inspector General of the U.S. Department of Labor. Any information on computer matching activity or issues related to computer matching would be appreciated. Responses from readers about articles appearing in the *Computer Matching* newsletter will also be welcome. Information should be sent to:

Camille Robinson
The Council of State Governments
P.O. Box 11910, Iron Works Pike
Lexington, Kentucky 40578
(606) 252-2291

(Continued from page 1)

dates of birth, of the recipients on each state's list with the recipients on each of the other seven states' lists. Out of 3.3 million names matched, 6,557 were raw hits—0.2 percent of the total.

Project coordinators for each state received a list of their state's food stamp recipients who appeared on other states' rolls. They then screened the entries, eliminating cases in which the Social Security numbers were incorrect or persons eligible for benefits did not actually collect their food stamps for the month. Screening reduced the matches by 26 percent, leaving 4,521 matches to be investigated.

The states spent three months investigating and documenting cases of duplicate participation. They submitted their results to the Southeast Regional Office of the U.S. Department of Agriculture's Food and Nutrition Service (FNS), the federal agency with oversight authority for the food stamp program. FNS staff compiled and analyzed the findings and will issue a report in the near future.

The states hope that the project's findings will help them discover answers to questions, such as: Where is duplicate participation occurring—just in border counties of neighboring states or in widely separated locations? What are the common characteristics of the persons committing this type of violation? What is the most cost-effective way to curb or eliminate the problem?

Prior to this match, there had been a number of matches to detect duplicate food stamp participation between neighboring states or in selected adjacent counties in neighboring states, but no widespread check had been conducted. This multistate effort should identify trends with universal applicability.

For more information, contact Cherie Morris, Regional Director, Family Nutrition Programs, USDA/FNS, 1100 Spring St., Atlanta, GA 30367, (404) 881-4981 (FTS 8-257-4981).

PCIE looks at inspection activities of inspectors general

Recently, the Prevention Committee of the President's Council on Integrity and Efficiency (PCIE) surveyed the prevention activities in the Inspector General (IG) community. One prevention activity conducted by the IG community is the "inspection." This past September, the PCIE prevention committee published its findings in the *Report on Inspections Activities of the Inspectors General.*

An inspection was defined, for the PCIE survey, as "any independent, objective examination (other than an audit or investigation) of a federal activity or program conducted by Inspector General staff to evaluate the effectiveness and economy of operations; compliance with laws and regulations; and/or the effectiveness of techniques to detect and prevent fraud, waste, and mismanagement. . . . Furthermore, an inspection is *generally* of *relatively* brief duration and results in a written report and/or oral briefing for senior management officials with specific recommendations on how to improve overall management of the activity or program."

The survey objectives were to query all statutory IGs to establish an inventory of ongoing inspection activities for wider application within the IG community and to highlight some of the more effective practices for consideration by all IGs. Based on this evaluation, a set of basic conditions essential for a successful inspection program was proposed.

One major finding was the unique difference between traditional IG activities—audits and investigations—and the more recent IG activity—inspections. The report states, "Inspections differ from audits and investigations in several aspects, the major differences having to do with purpose and objectives, scope and depth of coverage, adherence to standards, rigorousness and methodology, level and type of resources, and the level of involvement by program managers."

Moreover, the report states that, "Inspections evolved to satisfy important needs which were not being addressed by audits and investiga-

(Continued on page 8)

POINT COUNTER POINT

The following edited summary of remarks on the pros and cons of computer matching is based on two articles that appeared in the June 1984 issue of Communications of the ACM. John Shattuck, executive director of the Washington Office of the American Civil Liberties Union (ACLU), argues that "Computer Matching Is a Serious Threat to Individual Rights." In his article, Richard P. Kusserow, Inspector General at the U.S. Department of Health and Human Services (HHS), argues that "The Government Needs Computer Matching to Root Out Waste and Fraud."*

*Copyright, 1984, Association for Computing Machinery, *Communications of the ACM*, June 1984. Copying is by permission of the ACM.

John Shattuck

Computer matching provides a revolutionary method of conducting investigations of fraud, abuse, and waste of government funds. However, matching raises profound issues concerning individual privacy, due process of law, and the presumption of innocence.

To understand the impact of computer matching on individual rights, it is first necessary to grasp the difference between a computer-matching investigation and a traditional law enforcement investigation. A traditional investigation is triggered by some evidence that a person is engaged in wrongdoing. Our constitutional system bars the government from investigating persons it does not suspect of wrongdoing. A computer match is not bound by these limitations. It is directed not at an individual, but at an entire category of people.

A computer match is initiated not because any person is suspected of misconduct, but because his or her category is of interest to the government. What makes computer matching fundamentally different from a traditional investigation is that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin. That evidence is produced by "matching" two sets of personal records compiled for unrelated purposes.

Computer matching erodes four basic individual rights: the Fourth Amendment to be free from unreasonable search, the right to the presumption of innocence, the right to due process of law, and the right to limit the government's use of personal information to the purposes for which it was collected. Moreover, the rapid and unchecked growth of computer matching leads inexorably to the creation of a de facto national data system in which personal

(Continued on page 4)

Richard P. Kusserow

More information will be collected, stored, and retrieved in our lifetime than in all other generations combined. This information explosion, however, is creating new problems for the government managers. Crucial issues revolve around the use of computer technology to ensure that taxpayers' money is being safeguarded and to manage personal data without sacrificing individuals' rights to privacy.

Without the computer, government could not fulfill many mandated missions. Computers are here to stay and will become even more pervasive. We are witnessing the virtual disappearance of hard copy, a development of special importance to the government manager, auditor, and investigator.

Computer matching is an efficient and effective technique for coping with today's expensive, complex, and error-prone government programs. For instance, computer matching and other innovative techniques helped my office, the U.S. Department of Health and Human Services (HHS), identify $1.4 billion in savings—almost a 300 percent increase over the previous year.

Simply defined, computer matching is a technique whereby information within two or more records or files is compared to identify situations that could indicate program ineligibility or payment errors. The process, however, should not and does not stop there. The computer does not decide who is getting erroneous payments and does not automatically decide who should be terminated from the payment rolls. The computer merely provides a list of items that could indicate an erroneous or aberrant situation. The matched items must be investigated by program staff. Only then can an

(Continued on page 4)

Shattuck continued

data are widely and routinely shared at all levels of government and in the private sector.

The Office of Management and Budget (OMB) guidelines have rendered meaningless the central principle of the Privacy Act. The guidelines contain no requirements or limitations on the conduct of computer matching in these areas: the nature of the record systems to be matched; the procedures to be followed in determining the validity of the "hits"; the standards and procedures to be followed for securing OMB approval of a proposed match; and the projected costs and benefits of a proposed match.

As a general framework for safeguarding individual rights, I propose the following:

1. **The Privacy Act should be amended to clarify that computer matches are not ipso facto "routine uses" of personal record systems.**
2. **No further federal computer matches should be permitted without express congressional authorization.**
3. **Congress should not authorize computer matches of sensitive personal records systems (the confidentiality of which is otherwise protected by statute) such as taxpayer records maintained by the IRS, census records maintained by the Census Bureau, or bank records maintained by federally insured banking institutions.**
4. **No computer match should be authorized unless and until an analysis has been made of its projected costs and projected savings in the recoupment of funds owed to the government. The match should not be authorized unless the public benefit will far outweigh the cost—and unless individual rights will be protected. The results and full costs of any match should be published.**
5. **Procedural due process protections for the persons whose records are to be matched should be specified by statute, including the right to counsel, the right to a full hearing, and the right to confidentiality of the results of a match.**

I recommend a moratorium on all further matching so that Congress and the public can study the results of all computer-matching programs conducted to date and assess the long-term consequences. ★

Kusserow continued

agency determine whether a payment should be adjusted or stopped, or the file record corrected.

The overall objective of the President's Council on Integrity and Efficiency (PCIE) is to expand the cost-effective use of computer-matching techniques that prevent and detect fraud, abuse, and erroneous payments and, at the same time, to protect the rights and privacy of individuals. So far the project staff have inventoried federal and state matches, established a clearinghouse and a newsletter, and launched an effort with eight states to test standardized data extraction formats for computer matching. The standardized formats will make matching "hits" more reliable, thereby reducing the need for manual review of client files.

A common misconception is that computer matching is primarily an investigative tool. In reality, matches are used primarily to assist in government audits to identify inappropriate data (e.g., mistakes or errors) in the records under review. Most of the computer-assisted audits use computer screens rather than tape-to-tape matches, which are usually performed on a one-time basis. The information produced by a matching program is no different from that produced by any other audit or law enforcement inquiry. Once that is recognized, the constitutional concerns raised by Mr. Shattuck can be put into perspective.

Criticisms made against computer matching are generally unfounded. I strongly oppose Mr. Shattuck's recommendations as being unnecessary and inappropriate. His intent is to restrict, if not totally eliminate, the use of computer-matching projects by the federal government.

Requiring congressional authorization for each match and affording persons whose records are being matched rights far in excess of those available to the actual subjects of a law enforcement inquiry would not improve, but would end, the use of matching. This is far too vital an audit technique to lose, especially in view of the fact that Mr. Shattuck has failed to provide even a single example of a federal computer match that violated an individual's legal rights. ★

Matching adds taxpayers to NYC tax rolls and $$$ to city coffers

The city of New York has collected $75.9 million in back taxes due since it began a matching program in 1981. As of June 30 this year, 92,720 taxpayers had been added to the city's tax rolls.

The strategy of the city's Department of Finance, which conducts the computer matches, is to send questionnaires to potential non-filers uncovered by the matches. Since the matching program began, 818,401 potentially non-filing taxpayers have received questionnaires about their filing status. If the recipient does not respond after three questionnaires have been sent, an estimated notice of tax due is sent.

The city's Department of Finance primarily matches its own files and files of taxes administered by New York state against each other, or against other city data, such as files of licensees and contractors. Access to federal tax data, available to states, is prohibited. The department is also precluded from using New York state non-tax data unless it is available under the Freedom of Information Act.

The following computer matches are in effect:

- Corporation or unincorporated business tax files were matched against commercial rent tax (CRT) files to determine who had not filed CRT returns (the city levies an occupancy tax on commercial tenants who pay over $11,000 in rent). The result has been an additional 17,690 CRT taxpayers paying $24.8 million.
- Information returns from landlords were computerized and compared to lists of tenants and rent amounts in the CRT file; $7.3 million in back taxes have been collected from 1,887 taxpayers.
- The names of subtenants were extracted from the CRT file to see whether they had filed returns; $1.4 million has been collected from 154 taxpayers.
- CRT filers were matched against business tax filers—a reverse of the first match—to see which of the former had not filed business tax returns. A total of 3,695 taxpayers have paid $11.3 million.
- A tape of the city personal income tax was scrutinized for those who declared business income (Schedule C), and this data was matched against business tax files. Taxes of $2.4 million have been collected from 1,830 taxpayers.
- Sales tax tapes are being matched against business tax files to determine which taxpayers have not filed the latter returns; 4,337 taxpayers have remitted $1.5 million.
- A tape of doctors and other health practitioners who have permits for X-ray equipment has been matched against business tax and commercial rent tax files; 621 taxpayers have paid $353,305 in back taxes.
- Questionnaires were sent to 84,887 taxpayers who previously filed CRT returns but who had not filed such returns in one or more subsequent years. This has resulted in the collection of $6.7 million from 12,236 taxpayers.
- More than 430,000 taxpayers who filed business tax returns in 1976, but not in one or more of the subsequent years, were sent questionnaires. The result has been payment of $20.2 million by 50,270 taxpayers.

In addition to repeats of matches currently in process, new computer match programs will focus on consultants, vendors, contractors, and others who do business with the city government to determine whether they are paying the proper amount of business taxes.

For more information, contact Betsy Seidman, New York City Department of Finance, Room 506, Municipal Bldg., 1 Centre St., New York, NY 10007, (212) 566-5475.

New Jersey begins wage reporting

The New Jersey Department of Labor is now authorized to cross match claims for unemployment insurance (UI) against files from the state's Department of Human Services. Under the new amendments to the New Jersey unemployment compensation law, the department is also authorized to collect and utilize wage data in the processing of claims for UI.

The data is to be collected on a quarterly basis from all employers subject to the statute. Employee data elements include: (1) names of employees, (2) Social Security numbers, (3) gross wages paid during the quarter, and (4) the "base weeks" accrued by the employee during the quarter. A base week is defined as "any calendar week (Sunday through Satur-

(Continued on page 6)

Wisconsin tests standard formats

An innovative program to test the use and value of federal standardized formats in computer matching has been implemented in Wisconsin. In July 1983, the Wisconsin Department of Health and Social Services entered into a cooperative agreement with the Office of the Inspector General, U.S. Department of Health and Human Services. Wisconsin is testing the assistance programs and unemployment insurance formats.

Standard formats, predetermined arrangements of like data on file to facilitate extraction of data from other files by computer matching, were developed by the President's Council on Integrity and Efficiency (PCIE).

Wisconsin staff are testing the formats of the Wisconsin income maintenance files against:

- Wisconsin unemployment insurance files on a monthly basis.
- Illinois Department of Labor unemployment insurance (UI) files.
- Iowa income maintenance files.
- Minnesota unemployment insurance (UI) files.
- Internet data.

Wisconsin's development of a standard format tape of income maintenance matching files required 15 hours of programming time, for an approximate cost of $400. Minnesota did not convert its UI files to the standardized format; instead, a computer program was developed to match the Wisconsin files and provide output in the standard format. The match with Minnesota cost $1,480. This figure includes writing a program, 70 hours of programming time, computer run time and hard copy output. This first match with Minnesota was then repeated. The cost for the second match was only $104.50, plus a very small charge to create and send a second standard format case load tape to Minnesota.

The future suggests several possibilities for expanded use of standardized formats in computer matches. Individual states creating standard format tapes and developing programs to accommodate the tapes will facilitate interjurisdictional matches. For example, because Iowa converted its income maintenance files into the standard formats, the state can now match with the Minnesota Department of Economic Security, the Wisconsin Department of Health and Social Services, and the Illinois Department of Labor. As more states adopt the formats, the potential for matches between states will be unlimited.

For additional information, contact Ken Shimota, Fraud Manager, or Judy Sievers, Assistant Standard Format Project Director, Wisconsin Department of Health and Social Services, Room 384, P.O. Box 7851, 1 West Wilson, Madison, WI 53707, (608) 266-0606 or (608) 266-9964.

(Continued from page 5)

day) in the reportable quarter during which the employee earned remuneration from an employer equal to or greater than 15 percent of the statewide average weekly remuneration." Beginning October 1, 1985, such remuneration must equal or exceed 20 percent of the statewide weekly remuneration.

Actual use of the collected wage data for monetary determination in the unemployment insurance program will begin with claims filed on or after July 1, 1986. Cross matching of data between the unemployment insurance program and public assistance programs of the state's Department of Human Services began in November 1984.

The first reporting period was for the third calendar quarter of 1984 with a report due date of October 30, 1984. Each subject employer was issued a report package containing Form WR-30, "Employer Report of Wages Paid," a continuation page for employee listings, and complete filing instructions. Employers have the option of either returning the hard-copy WR-30 form and any continuation sheets required, or with prior approval, submitting their reports via magnetic tape. To date, over 90 organizations, representing nearly 8,000 employers, have submitted their data on magnetic tape. All other returns are keyed into the automated system.

Questions on New Jersey's wage reporting programs should be directed to Larry J. Crider, Assistant Director of Finance, Department of Labor, 1206 Labor Bldg., Trenton, NJ 08625-0078, (609) 292-0165.

California conducts four-way standard formats demonstration

A demonstration project has been initiated to test and evaluate the feasibility and cost-effectiveness of applying the federal standardized formats to automated matches currently being conducted in California. The demonstration project is a cooperative venture of the California Department of Social Services and the Office of Inspector General (OIG), U.S. Department of Health and Human Services.

Another purpose of the demonstration project is to test for the feasibility of detecting AFDC recipients who list non-existent children on their claims to qualify for the AFDC program. The population group of the standardized format master files includes all children under six years of age in Santa Clara County with a reported Social Security number whose families are currently on AFDC.

The standardized format project master file was created by extracting data from the Santa Clara social services master file and converting the data to the standardized format. Four matches were then performed between the master file and a death index (six years), Medi-Cal paid claims (18 months), birth index (six years), and child support payment files. Results of these matches were assigned weights and then merged into one file.

A total of 3,573 cases in a population of 16,031 were identified as possible suspects. These cases then went to the Social Security Administration (SSA) for Numident verification processing to identify those records with invalid Social Security numbers. The most suspicious cases were then forwarded to Santa Clara County for follow-up investigations.

The master file was created, all four matches were completed, and match results were merged by October 31, 1984. California is now reviewing the results of the Numident verification before investigations begin. For additional information, contact Larry Harrison, State Project Officer, Welfare Fraud & Audit Bureau, Department of Social Services, 744 P St., MS19-28, Sacramento, CA 95814, (916) 924-2828.

Update on Integrated Quality Control Data Processing System

The state and federal governments now have a national data base on quality control, the Integrated Quality Control Data Processing System (IQCDPS). The system is serving state and federal agencies in the administration of AFDC, Medicaid, and food stamp programs. For many states, this system provides analytical capability that they previously did not have.

All the states provide data for the Washington Computer Center. States not only enter and edit data, but can also produce error-prone profiles, perform analyses of programs, and produce federally required quality control reports. An added benefit of the system is its capacity to perform generic reviews of integrated programs and single systems instead of separate reviews of each program.

Since October 1, 1982, state welfare agencies have been able to enter data into the host computer at the USDA Washington computer center. Federal agencies can access this national data base. The Office of Family Assistance (OFA) and the Food and Nutrition Service (FNS) have trained regional office personnel and program staff to respond more effectively to state inquiries on the operations and maintenance of the IQCDPS.

The IQCDPS is managed by a committee, chaired by the director of the Office of Public and State Data Systems, HHS. Commitee members represent the OFA, the FNS, the Health Care Financing Administration, and state quality control directors.

The management committee addresses various problems and proposes solutions to improve the operation of the IQCDPS. For example, state hardware capability will be improved by the procurement of upgraded equipment. A federal contract will be awarded to deal with the problems of IQCDPS software and with issues surrounding the host computer environment. The management committee also plans to contract for the maintenance and improvement of the IQCDPS during fiscal year 1985.

For more information, contact Karl Piekarski, Office of State Operations, Office of Family Assistance, USDHHS, 2100 2nd St., S.W., Washington, D.C. 20201, (202) 245-2017.

(Continued from page 2)

tions. The most notable of these are the needs to fill the audit 'void' and provide greater coverage with less staff, generate deterrence through greater IG coverage, provide timely feedback to program managers about the problems, review new operations early in their existence, and provide leads or referrals for audits and investigations. Although many IGs believe there is a distinct class of review activity separate and apart from audits and investigations which evolved to address different needs, within that class there are many variations on a theme. . . . OIGs using inspections believe that the real advantage of inspections over other review methods is flexibility. This flexibility has resulted in the development of many innovative techniques and approaches."

In addition to identifying the differences between inspections and other IG activities, the report discusses the institutionalization of the inspections role in the IG community; the important needs served by inspections; variations among agencies conducting inspections; and some impressive accomplishments resulting from inspections activities.

The report indicated that, although inspections are a relatively new and still-evolving activity, they have already achieved impressive results in program efficiencies, program capacity enhancements, cost savings, and referrals for audits and investigations. Most IGs with established inspection functions are pleased with the benefits from inspections, according to the report.

The *Report on Inspections Activities of the Inspector General* is a significant contribution to the PCIE prevention efforts and to the existing literature on IG activities. The PCIE Long Term Computer Matching Project Committee is pleased to share some of the highlights with readers of *Computer Matching*. Questions about the study and requests for copies of the report should be directed to: Joseph Sherick, Inspector General, Department of Defense, Chairman, PCIE Prevention Committee, Washington, D.C. 20301, (202) 695-4249.

U.S. Department of Health and Human Services
Office of Inspector General
Washington, D.C. 20201

Official Business
Penalty for Private Use, $300

THIRD-CLASS MAIL
POSTAGE & FEES PAID
DHHS
PERMIT No. G-45

Computer Matching

Privacy Act Considerations

1. Creating new or altered systems of records

a. The public has a right to know what records are being maintained and a right to assure their accuracy.

b. New or altered systems of records must be reported to Congress and OMB through General Counsel before creation of the file.

c. No clear definition exists for "new or altered system of records" as it applies to combining computer files for a match project when these new files exist only temporarily as a work product in a project case.

2. Using an existing system of records for a new purpose not previously advertized in Federal Register.

a. Personnel type records have extensive routine use and can generally be used for computer match activities involving other agencies.

b. Tax records have no routine use descriptions and cannot be generally used except as provided for tax administration (IRC 6103).

c. No clear determination has been made concerning investigative disclosures of tax information in a computer match project. However, it appears this avenue may be legitimate as long as we are making the disclosure solely to obtain information to complete our own investigations; not to provide other federal or state agencies with information for their investigations.

d. Notice of new or modified use must be published in the Federal Register 30 days prior to the new use to provide an opportunity for interested persons to comment.

3. c. Disclosure of records in a computer match must be compatible with the purpose for which the records were originally collected.

Accounting for disclosures

a. Agencies must be sure to maintain an accounting of the disclosure made through a computer match in accordance with 552a(c) of the Privacy Act.

OMB Matching Guideline Requirements

1. Brief public notice of computer match should be published in the Federal Register as close as possible to the initiation of the matching program. A copy of this notice should be sent to Congress and OMB at the same time.

2. Each match must be documented in an annual report to OMB.

3. Disclosure of computer match records to either a federal or non-federal entity should be preceded by a written agreement governing the conditions of the use, disposition, and security of the matching file.

Computer Matching Project Plan

I. Identify match area

- A. Participating agencies
- B. Files to be matched
- C. Key data elements
- D. Match criteria
- E. Eligibility requirements for benefits
- F. Potential for fraud
- G. Legal considerations

II. Develop a comprehensive plan -

- A. Resources needed
  1. Data and files
  2. Staff
  3. Processing - hardware and software
  4. Follow-up needs
- B. Legal requirements
  1. Privacy Act issuances if needed
  2. Federal Register announcement - OMB guidelines
- C. Documentation - to be used in annual report to OMB
  1. Overall plan
  2. Agreements between agencies
  3. Federal Register announcements
  4. Computer programs and files used
  5. Eligibility rules
  6. Agreed policies and criteria
  7. Results
  8. Problems encountered and solutions

III. Perform Match

- A. Security considerations
- B. Refine criteria for cost-effective results

IV. Pursue Hits

- A. Prioritize hits
- B. Prosecution considerations

V. Follow-up

- A. Analyze cause of problems identified by match
- B. Implement preventive measures

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-82-5

May 11, 1982

MEMORANDUM FOR THE EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

FROM: David A. Stockman
Director

SUBJECT: Revised Supplemental Guidance for Conducting Matching Programs

I am attaching a copy of our revised Guidelines on conducting computerized matching programs. This revision updates and simplifies earlier guidance issued on March 30, 1979. It is effective immediately.

The revision is the result of our evaluation of agencies' operating experiences under the original Guidelines. The new Guidelines incorporate many agency recommendations for clarifications and changes. In addition, they greatly simplify the notice and reporting requirements of the earlier version.

Direct comments or questions on these Guidelines to OMB's Office of Information and Regulatory Affairs.

Attachment

Matching Guidelines

1. Purpose - These Guidelines supplement and should be used in conjunction with the "OMB Guidelines on the Administration of the Privacy Act of 1974," issued on July 1, 1975 and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concerns expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." These Guidelines do not authorize activities which are not permitted by law; nor do they prohibit activities expressly required to be performed by law. Complying with these Guidelines, however, does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these Guidelines.

2. Scope - These guidelines apply to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a), and to all matching programs:

   a. Performed by a Federal agency, whether the personal records used in the match are Federal or non-Federal.

   b. For which a Federal agency discloses any personal records for use in a matching program performed by any other Federal agency or any non-Federal organization.

3. Effective Date - These guidelines are effective on their date of issuance - May 11, 1982.

4. Definitions - For the purposes of these Guidelines:

   a. All the terms defined in the Privacy Act of 1974 apply.

   b. A "personal record" means any information pertaining to an individual that is stored in an automated system of records, e.g., a data base which contains information

about individuals that is retrieved by name or some other personal identifier.

c. A "matching program" is a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants.

Matching Programs do not include the following:

(1) Matches which do not compare a substantial number of records, e.g., comparison of the Department of Education's Defaulted Student Loan data base with the Office of Personnel Management's Federal Employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

(2) Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

(3) Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

(4) Matches done to produce aggregate statistical data without any personal identifiers.

(5) Matches done to support any research or statistical project where the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

(6) Matches done by an agency using its own records.

d. A "matching agency" is the Federal agency which actually performs the match.

e. A "source agency" is the Federal agency which discloses records from a system of records to be used in the match. Note that in some circumstances, a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match. The disclosure

proceed to make the disclosure to the matching agency. It should ensure that only the minimum information necessary to conduct the match is provided. If disclosure is to be made pursuant to a "routine use" (Section (b)(3) of the Privacy Act), it should ensure that the system of records contains such a use, or it should publish a routine use notice in the Federal Register. The agency should also be sure to maintain an accounting of the disclosures pursuant to Section (c) of the Privacy Act.

(2) To a Non-Federal Entity - Prior to disclosing records to a non-Federal entity for a matching program to be carried out by that entity, a source agency should, in addition to all of the considerations in 5a(1) above, also make reasonable efforts, pursuant to Section (e)(6) of the Privacy Act, to "assure that such records are accurate, complete, timely, and relevant for agency purposes."

b. Written Agreements - Prior to disclosing to either a Federal or non-Federal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file, e.g.: that the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file(s) previously agreed to; that it will not be used to extract information concerning "non-hit" individuals for any purpose; and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency.

c. Performing Matching Programs -

(1) Matching agencies should maintain reasonable administrative, technical and physical security safeguards on all files involved in the matching program.

(2) Matching agencies should insure that they have appropriate systems of records including those containing "hits," and that such systems and any routine uses have been appropriately noticed in the Federal Register and reported to OMB and the Congress as appropriate.

d. Disposition of Records -

(1) Matching agencies will return or destroy source matching files (by mutual agreement) immediately after the match.

(2) Records relating to hits will be kept only so long as an investigation, either criminal or administrative, is active and will be disposed of in accordance with the requirements of the Privacy Act and the Federal Records Schedule.

e. Publication Requirements -

(1) Agencies, prior to disclosing records outside the agency, will publish appropriate "routine use" notices in the Federal Register, if necessary.

(2) If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, the agency involved should publish the appropriate Federal Register notice and submit the requisite report to OMB and the Congress pursuant to OMB Circular No. A-108.

f. Reporting Requirements -

(1) As close to the initation of the matching program as possible, matching agencies shall publish in the Federal Register a brief public notice describing the matching program. The notice should include:

(a) The legal authority under which the match is being conducted;

(b) A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose(s) for which the program is being conducted, and the procedures to be used in matching and following up on the "hits";

(c) A complete description of the personal records to be matched, including the source(s), system of records identifying data, date(s) and page number(s) of the most recent Federal Register full text publication where appropriate;

(d) The projected start and ending dates of the program;

(e) The security safeguards to be used to protect against unauthorized access or disclosure of the personal records; and

(f) Plans for disposition of the source records a "hits."

Agencies should send a copy of this notice to the Congress and the Office of Management and Budget at the same time it is sen

(2) Agencies should report new or altered systems of records as described in e (2) above as necessary.

(3) Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and the government's effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by Section (p) of the Privacy Act or Section 3514 of P.L. 96-511.

g. Use of Contractors - Matching programs should, as far as practicable, be conducted "in-house" by Federal agencies using agency personnel, rather than by contract. When contractors are used, however,

(1) The matching agency should, consistent with subsection (m) of the Privacy Act, cause the requirements of that Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by FPR Amdt. 155, 41 CFR 1-1.337-5;

(2) The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards and guidelines issued by OMB, GSA, and the Department of Commerce;

(3) The terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use;

(4) Contractor personnel involved in the matching program should be made explicitly aware of their obligations under the Act, and of these guidelines, agency rules and any special safeguards in relation to each specific match performed.

(5) Any disclosures of records by the agency to the contractor should be made pursuant to a "routine use" (Section (b)(3) of 5 U.S.C. 552a).

6. Implementation and oversight - the Office of Management and Budget will oversee the implementation of these Guidelines and shall interpret and advise upon agency proposals and actions within their scope, consistent with Section 6 of the Privacy Act.

INVESTIGATIVE NOTE: IDENTIFYING "800" TELEPHONE ACCESS NUMBERS

(REPRINTED FROM THE JANUARY 1985 ISSUE OF NARCOTICS NEWSLETTER)

More and more frequently, drug traffickers and money launderers are utilizing specialized communications systems (e.g., telexes and electronic mail) in the course of their criminal activities. (See related "investigative notes" in the October and November-December 1983, and the March, August, and November-December 1984 issues of the NARCOTICS NEWSLETTER.) When law enforcement agents are investigating drug-related activity, they should give special attention to "800" numbers captured by Dial Number Registers ("pen registers") because many of the specialized communications systems referred to above are accessed by use of such toll-free "800" telephone numbers. By providing its customers with toll-free access to these lines, the communications companies have also provided the unintended benefit of allowing national and international communications without the creation of traditional telephone toll records (see the November-December 1984 NARCOTICS NEWSLETTER) and, at the same time, have removed any necessity to obtain specialized leased circuits or lines. Because local telephone companies will, in most cases, not be able to identify the subscribers of "800" numbers (including access numbers and other types of toll-free service), investigators should first attempt subscriber identification by contacting AT&T Communications and requesting to speak with a local security officer. A subpoena will, of course, be required to identify the subscribers of all non-published numbers. A numerical "watch list" of some of the "800" telephone numbers used to access several of the more popular communications systems is set forth below.

Phone number	Common Carrier and Service
800-221-2896	FRENCH TELEGRAPH CABLE COMPANY S&F TELEX (300)
800-221-3623	ITT WORLDWIDE COMMUNICATIONS REAL TIME TELEX (300)
800-221-9455	FRENCH TELEGRAPH CABLE COMPANY TELEX MAIL BOX (300)
800-221-9954	ITT WORLDWIDE COMMUNICATIONS S&F TELEX (110/300/1200)
800-222-0555	TYMNET PUBLIC DATA (PACKETT SWITCHED) NETWORK
800-223-3445	WESTERN UNION INTERNATIONAL (MCI) TELEX
800-231-2300	FRENCH TELEGRAPH CABLE COMPANY S&F TELEX (1200)
800-231-3677	FRENCH TELEGRAPH CABLE COMPANY TELEX (110)
800-323-0905	MCI MAIL (ELECTRONIC MAIL WITH TELEX ACCESS)
800-323-6397	WUT. CO. EASYLINK FYI SERVICE (110)
800-325-4050	EASYLINK (ELECTRONIC MAIL WITH TELEX ACCESS) (110)
800-325-4112	EASYLINK (ELECTRONIC MAIL WITH TELEX ACCESS) (300/1200)
800-325-6397	WUT. CO. EASYLINK FYI SERVICE (300/1200)
800-368-3343	SOURCE TELECOMPUTING CORPORATION (ELECTRONIC MAIL)
800-368-5963	ALLNET LONG DISTANCE TELEPHONE SERVICE
800-424-4325	TRT TELECOMMUNICATIONS REAL TIME TELEX (110)
800-424-9494	TELENET PUBLIC DATA (PACKETT SWITCHED) NETWORK
800-446-4462	SBS SKYLINE LONG DISTANCE TELEPHONE SERVICE
800-522-3833	ITT WORLDWIDE COMMUNICATIONS REAL TIME TELEX (NY) (300)
800-526-3612	RCA GLOBAL COMMUNICATIONS S&F TELEX (1200)
800-526-3714	RCA GLOBAL COMMUNICATIONS REAL TIME TELEX (300)
800-526-3881	RCA GLOBAL COMMUNICATIONS S&F TELEX (300)
800-572-3517	SOURCE TELECOMPUTING CORPORATION (ELECTRONIC MAIL) (VA)
800-624-1022	MCI LONG DISTANCE TELEPHONE SERVICE
800-654-2224	ITT WORLDWIDE COMMUNICATIONS REAL TIME TELEX (300)
800-662-1700	NETWORK PLUS LONG DISTANCE TELEPHONE SERVICE
800-821-6629	LEXITEL CORPORATION (MAX LONG DISTANCE TELEPHONE SERVICE)

Further information on this article and related subjects may be obtained from James R. Hastings, Special Attorney, Organized Crime and Racketeering Section, Criminal Division, FTS 633-3707, and Thomas A. Blair, Assistant United States Attorney, Southern District of Florida, FTS 350-5201.

DISTRICT OF COLUMBIA-METROPOLITAN AREA
LOCAL TELEPHONE NUMBERS
ACCESSING SPECIALIZED COMMUNICATIONS

347-3337	UNINET-PUBLIC DATA NETWORK (300/1200)
352-3136	TYMNET-PUBLIC DATA NETWORK (2400)
352-7500	COMPUSERVE (ELECTRONIC MAIL) (300/1200)
352-8750	COMPUSERVE (ELECTRONIC MAIL) (1200)
362-7754	ITT WORLDWIDE COMMUNICATIONS-TELEX SERVICE
429-0956	TELENET-PUBLIC DATA NETWORK (300/2400)
429-7800	TELENET-PUBLIC DATA NETWORK (1200)
429-7896	TELENET-PUBLIC DATA NETWORK (300)
448-9191	SOURCE TELECOMPUTING CORP. (ELECTRONIC MAIL) (300)
448-9440	SOURCE TELECOMPUTING CORP. (ELECTRONIC MAIL) (1200)
463-1800	ALLNET-LONG DISTANCE TELEPHONE SERVICE
479-4411	LEXITEL CORP.-MAX LONG DISTANCE TELEPHONE SERVICE
525-6500	MCI MAIL (ELECTRONIC MAIL WITH TELEX ACCESS)
565-4110	ITT LONGER DISTANCE-TELEPHONE SERVICE
638-7669	EASYLINK (ELECTRONIC MAIL WITH TELEX ACCESS) (1200)
638-7679	EASYLINK (ELECTRONIC MAIL WITH TELEX ACCESS) (300)
638-7694	EASYLINK (ELECTRONIC MAIL WITH TELEX ACCESS) (110)
652-0800	TYMNET-PUBLIC DATA NETWORK (1200)
691-8200	TYMNET-PUBLIC DATA NETWORK (1200)
691-8390	TYMNET-PUBLIC DATA NETWORK (1200)
728-0084	MCI TELECOMMUNICATIONS-LONG DISTANCE TELEPHONE
728-0124	U.S. TELEPHONE-LONG DISTANCE SERVICE
731-2051	UNINET-PUBLIC DATA NETWORK
737-2051	WESTERN UNION TELEGRAPH-LONG DISTANCE TELEPHONE
828-3700	AUTONET-PUBLIC DATA NETWORK
841-9834	COMPUSERVE (ELECTRONIC MAIL) (300/1200)
861-0301	NETWORK PLUS-LONG DISTANCE TELEPHONE SERVICE
950-0777	GTE-SPRINT-LONG DISTANCE TELEPHONE SERVICE
950-1020	WESTERN UNION TELEGRAPH-LONG DISTANCE TELEPHONE
950-1022	MCI TELECOMMUNICATIONS-LONG DISTANCE TELEPHONE
950-1033	U.S. TELEPHONE-LONG DISTANCE SERVICE
950-1066	LEXITEL CORP.-MAX LONG DISTANCE TELEPHONE
950-1088	SBS SKYLINE-LONG DISTANCE TELEPHONE SERVICE

AO 106
Rev 6/82

AFFIDAVIT FOR SEARCH WARRANT

United States District Court

DISTRICT
Southern District of Georgia

United States of America
vs.

A two story dwelling house commonly known as 101 Palmetto Lane, Brunswick, Georgia

DOCKET NO.

MAGISTRATE'S CASE NO.

NAME AND ADDRESS OF JUDGE[1] OR FEDERAL MAGISTRATE
Hon. Marvin Highsmith
United States Magistrate
Federal Building
Brunswick, Georgia 31520

The undersigned being duly sworn deposes and says: That he/she has reason to believe that

☐ on the person of ☒ on the premises known as

DISTRICT
Southern District of Georgia

SEE ATTACHMENT 1

The following property is concealed:

SEE ATTACHMENT 2

Affiant alleges the following grounds for search and seizure[2]

Being property that constitutes evidence of, or property designed or intended for use or which has been used as a means of committing an offense against the United States in violation of 18 U.S.C. 641, 18 U.S.C. 912, and 18 U.S.C. 1030.

☐ See attached affidavit which is incorporated as part of this affidavit for search warrant

Affiant states the following facts establishing the foregoing grounds for issuance of a Search Warrant:

SEE ATTACHMENT 3

SIGNATURE OF AFFIANT

OFFICIAL TITLE, IF ANY

Sworn to before me, and subscribed in my presence:

DATE

JUDGE[1] OR FEDERAL MAGISTRATE

[1] United States Judge or Judge of a State Court of Record.
[2] If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure 41(c), show reasonable cause therefor

ATTACHMENT 1

The dwelling house located at 101 Palmetto Lane, Brunswick, Georgia, a two story brick house with white shutters. The numbers "101" are fastened to the left side of the front door. There is a driveway that begins at Palmetto Lane and circles around to the back of the house. In the front yard is an oak tree that is approximately 50 feet tall. Hanging from one of the lower branches of the tree is a rope swing. At the street directly in front of the dwelling is a mail box with the name "Marcelus" printed on it.

ATTACHMENT 2

Computers, keyboards, central processing units, external drives and/or external storage, tape and/or disks, terminals and/or video display units and/or receiving devices and peripheral equipment such as, but not limited to, printers, automatic dialers, modems, accoustic couplers; Unit 5150 IBM Personal Computer, 5201 Quietwriter printer, 3863 model 2 modem; journals, ledgers, customer listings, diaries, logs and other records, correspondence, momoranda, telephone and communications service billing information, computer software, programs and source documentation, computer logs, historical data for the period from January 1, 1985 through the present, flowcharts, block diagrams, assembled or partially assembled computer programs, and operating instructions; which have been used or are fit for use in the obtaining, maintenance, dissemination, and/or sale of confidential information obtained from the files of the United States Criminal Investigative Service; the means and instruments of obtaining, maintaining, disseminating and/or sale of such information; and other evidence of the offense.

ATTACHMENT 3

I am a Special Agent with the United States Criminal Investigative Service (CIS) assigned to the Brunswick, Georgia office. I have held this position for the past five years. As a CIS Special Agent I have the authority to investigate any alleged offenses against the United States, and make arrests for federal misdemeanors committed in my presence and federal felonies based upon probable cause. I am also authorized by statute to execute search warrants in the course of my investigations.

On July 5, 1985, at 9:35 a.m., a man entered my office in an extremely agitated state. This man has provided me with reliable information in excess of four times in the past which has proven extremely valuable to my investigations. He was the primary source of information in a recent successful investigation involving a person by the name of Barbara Johnson.

My informant told me that the previous night while he was eating dinner, a man known to him as Jeffrey Ward telephoned him and said that if he ever saw him again, he would kill him. Ward said that he had heard that my informant was a government informant, that he had "ratted on" Barbara, and that he had provided information to the government on four other occasions which had resulted in the arrest and conviction of drug traffickers. My informant said he denied the whole thing but Ward refused to believe him. Before hanging up, Ward told my informant that he could find out who the informers were and what they were telling the "feds" any time he wanted to.

I contacted a few of my other informants to find out if they had been similarly threatened. Each told me that he/she was becoming reluctant to cooperate with me anymore; that the drug dealers appear to know who the informers are and what information they are providing to the government.

CIS maintains their files in a computer system. One of the files in the system deals with CIS informants. Each informant is assigned a number which is used to retrieve the informant's record in the file. There is a separate record which contains the names of all of the informants and their identification numbers. Access to the computer system is available to all Special Agents and supervisory personnel. Access to the informant file is restricted to the Chief, Records Branch, and her two assistants, Robert Clark and Wanda Devore. To gain access to the computer system requires the requestor to enter an access code and a password. Each time an informant provides information, an entry is made in the informant's record showing the time and date the information was

provided, and a brief synopsis. At a later time, the record is updated to show whether the information proved correct and the disposition of the case.

The informant record file is maintained primarily to provide sources of information in future investigations. In addition, when the veracity of an informant is challenged at a suppression hearing, the file is used to bolster the informant's credibility.

One of the informants I spoke with has provided information during six prior drug investigations. Because this information proved instrumental in making my cases, I have a great deal of trust in him. He told me that he had talked with Ward on May 31, 1985 and that Ward had told him that he didn't have to worry any more about the "feds" because he could find out who was providing information to the government. My informant said he had asked how Ward could do this and that Ward had replied that a guy named "Marcelus" had access to the CIS computer and, for a price, would run a name check to see if a particular person was a CIS informant.

I was unfamiliar with a person named Marcelus, so, on July 7, I contacted another of my informants. This informant has proven reliable on five occasions in the past when I was looking for information during my investigations.

The informant told me that he knew a Keith Marcelus who ran a tax preparation and bookkeeping service out of his home for various local businesses and individuals in the area. According to the informant, Marcelus is also associated with the criminal element in the community. The informant said that he had been in Marcelus' home at 101 Palmetto Lane on June 15, 1985. Marcelus had bragged about his new business, had taken him down to the basement and had shown him an IBM PC and other computer equipment. The informant said that he had also seen boxes of computer disks on a shelf along the wall. Marcelus then said, "This baby can get into anywhere. The government has lots of good stuff in their computers. Why shouldn't we use computers to find out what the government has." Marcelus then typed something into the computer, the informant heard the sound of a telephone dialing, and the following log-on appeared on the screen.

* * * * *

UNITED STATES CRIMINAL INVESTIGATIVE SERVICE.
PLEASE ENTER YOUR NAME AND ACCESS CODE.

* * * * *

Marcellus then typed something else into the computer and the following message appeared:

* * * * *

PLEASE ENTER YOUR PASSWORD

* * * * *

Marcelus typed some more and received the following:

* * * * *

ENTER FILE NUMBER:

* * * * *

At this point, Marcelus turned off the computer and said, "I'm going to make enough money for Wanda and me to live in luxury forever. The money from my bookkeeping service is peanuts compared to what I can get with this." Picking up a 5¼" floppy disk, Marcelus said, "There ain't nobody who wouldn't pay to know what is in these files." Marcelus and the informant then left the basement, had a couple of beers, and the informant left.

On July 10, CIS changed their system so that all requests for information from the informant file were routed to a file containing information on fictitious individuals. CIS also had installed on their computer system a special feature known as the "WYLBUR Spy Function" which automatically records any requests made of the computer from a remote terminal. The "spy" also records the computer's responses to such requests before they are sent out over the telephone lines. On July 12, 1985, using the "spy" function, CIS determined that a request was being made from a remote terminal for information from the informant file. The request was made for a name check on one of the informants who have provided the above information to which the computer had returned a "File Not Found" response indicating there was no information on that person in the file.

On July 13, the "spy" alerted CIS officials that a request for information from the informant file was being made. My supervisor asked the telephone company to trace the line. The manual trace led to a telephone in Marcelus' home on Palmetto Lane.

On July 14, I visited Computerworld, a local IBM retailer. The Computerworld records indicated that on January 1, 1985 a Keith Marcelus had purchased the following:

(1)	Unit 5150, IBM PC, 256K w/ 2 disk drives	$1694.00
(2)	3863 Model 2 Modem	693.54

Washington Crime News Services'

COMPUTER CRIME DIGEST

PUBLISHED MONTHLY BY WASHINGTON CRIME NEWS SERVICES

Vol. 5 No. 1 January 1987 Page 1

THE SPECIAL CONSIDERATIONS OF COMPUTER SECURITY IN THE MICROCOMPUTER ENVIRONMENT

By Dr. Karen A. Forcht
Assistant Professor
James Madison University, Harrisonburg, Va.

It has been estimated that in another five years there will be over 500 million workstations in our business environments. This equates to a workstation for approximately every two or three employees. Many of these workstations will be comprised of microcomputers. Probably no other product has ever received such phenomenal growth and acknolwedgement of potential in terms of public awareness in recent years as the personal computer. IBM Corporation estimates that its gross annual sales will be nearly $4 billion this year. By itself as a product line, this represents a figure bigger than most major corporations' entire sales. (Schweitzer, 1986, p. 18)

Many organizations are now connecting their microcomputers to larger mainframes or linking them with local networks. In many cases, some of the organization's more sensitive and critical information now resides within these microcomputers. A few microcomputers in an organization today can conceivably have the same power that an entire data processing center had ten years ago.

(Continued on page two)

IN THIS ISSUE

MICROCOMPUTERS: Special Considerations Necessary For Security 1

REP.GLICKMAN: Reintroduces Computer Security Bill 5

IIA: Issues Statement Opposing DoD Information Restrictions 5

NEW INSTITUTE: Formed To Aid In Protection Of Information Assets 7

THE "CRACKER": Computer Hacker Still Being Sought 8

CALENDAR OF EVENTS 9

TELEMARKETING FRAUD: Joint Campaign Launched 9

PC SECURITY: Low Cost System Unveiled 10

Richard J. O'Connell, Publisher • **Susan M. Kernus**, Editor • **Nancy Van Wyen**, Subscription Director
7043 Wimsatt Road, Springfield, Virginia 22151–4070 Phone: (703) 941–6600
Single subscription $136 per year. Sample copies and multi-copy rates available upon request.

Copyright © by Washington Crime News Services. Reproduction in any form without the expressed written permission of the publisher is forbidden by the full penalties provided by the United States Copyright statutes.

Substantial Growth

From very limited beginnings, organizational computer use has grown substantially. Examination of statistics prepared by the International Data Corporation, a firm whose business is to study the computer industry, shows quite readily how widespread this growth has become:

- About 100,000 computer instructions are executed every second in the United States for each of its citizens.
- Each U.S. Citizen "appears" in 10 to 1,000 databases.
- Most homes have 2 to 10 "computers" (microprocessors).
- In the next five years, a trillion dollars will be spent in the U.S. on information processing.
- The information processing industry is growing at a yearly rate of 16 percent with many sizeable sectors growing at 25 percent or higher.
- By 1986, there will be over eight million computers installed in the United States, over 17 million terminals, and over five million word processing workstations.
- From 1971 to 1981, there was a fourfold growth in real dollars in the information processing industry.
- At the present growth rates, at the end of the decade of the '80s, there will be more than one intelligent office "gadget" for every white-collar worker. (Dickson and Wetherbe, 1985, p. 21)

During this rapid growth stage witnessed in the past decade, computers have proliferated in organizations of all sizes and types. Often, as this growth proceeded, security was not considered in the system design stages. According to Farr (1972, p. 36), "This attitude may well have resulted from lack of understanding by company management of the functioning of their computer systems and their peculiar vulnerability to novel forms of fraud and malicious interference."

Vulnerabilities

Microcomputers are presenting organizations with a whole new range of vulnerabilities and some unique problems connected to the old information security issues, including many of the following:

- "hackers"
- "piracy" of software
- end-user fraud
- industrial espionage
- integrity of the data being used for decision making
- modifying other users' files
- reading of another person's electronic mail
- power damage and theft

Losses resulting from microcomputer fraud, theft of machines and their components, and the stealing of software used on the microcomputers is now reaching epidemic proportions of well over a billion dollars a year.

Issues In Data Security

The nature of data – along with the necessary resulting measures – is of two distinct types and is derived from its use. Basically, these two attributes (types) apply: confidentiality and essentiality.

- **Confidentiality**

If some data concern a private party or person (e.g., client or patient), and if only certain persons are permitted access to it, it possesses a degree of confidentiality.

- **Essentiality**

If some data have a high degree of importance for a user such that, if lost through unintentional modification or theft it can be recovered only at a high expense, then it possesses a degree of essentiality (Madnick, 1975).

An example of the differentiation between the two types of data could be as follows:

A proprietary software package possesses high confidentiality because parties outside the vendor-buyer relationships are not allowed examinations or use of the package. Essentiality may be very high to the owner, whereas for the buyer, it is rather low (an extra copy can always be obtained). Zip codes have low essentiality because of their public nature and availability (Madnick, 1975).

Recent Violation

During the summer of 1983, seven youths ranging in age from 15 to 22 in the Milwaukee, Wisconsin area, gained access to computers spread across the United States and Canada. Penetration was made by the 414s (as the group called themselves after the Milwaukee area's telephone area code) into such vital computers as:

- Memorial Sloan-Kettering Center in New York City
- A bank in Los Angeles
- A cement company in Montreal, Canada
- An unclassified computer at a nuclear weapons laboratory in Los Alamos, New Mexico

According to Elmer-DeWitt, "The Sloan-Kettering Caper and this summer's hit movie (1983) *War Games* – the story of a young computer buff who nearly sets off a nuclear war when he accidentally gets into one of the Defense Department's most sensitive machines – have focused attention on a serious question: How to safeguard information stored inside the computer" (p. 34).

The potential for fraud is awesome. "The American banking system alone moves more than $400 billion between computers every day. (Elmer-DeWitt, 1983, p. 34). Corporate data banks hold consumer records and business plans worth untold billions. Military computers contain secrets that, if stolen, could threaten United States security (Elmer-DeWitt, 1983). Many of these machines are linked into the telephone system, which enables them to communicate with other computers and with users in remote locations.

The security problems that have long plagued the mainframe environment are now carrying over into the micro environment and special measures must be taken to ward off possible breaches before they occur.

Back-Up Procedures

The practice of using effective back-up procedures regularly should be followed. "Making copies of diskettes and tapes should be as routine as booting up the system" (Christie, p. 93). Since storage media can be damaged by fire, electrical fluxes in the power lines, mechanical failure, misuse, and operator error, back-ups are vital to an ongoing operation. The recommended practice is to have one copy available on the premises for immediate back-up and one stored off-site.

Disaster Recovery

"Disaster recovery probably began when the first operator ran over the first disk with his chair," said Thomas Braniff, senior consultant at Elasco Risk Management Consultants in New York City. "Whoever that first operator was, his descendants are legion," according to a recent article entitled "Protect Yourself From Crime" in *Business Computer Systems* (October, 1982). High on the list of accidental causes of data loss in the small system environment are disk damage and disk erasure. The floppy disk is susceptible to damage resulting from cigarette smoke, staples, magnets, and moisture. Even when the hazards are known, it is not always easy to avoid them so a disaster recovery system should be set up to work in conjunction with the back-up procedures. Some of the common hazards found in today's office are:

- **Sunlight** can be extremely damaging to a disk. Avoid placing disks on window sills.
- **Static electricity**. A non-static rug should be placed in the computer area to avoid static build-up.
- **Cigarette smoke**. Smoke can interfere with the reading of data by the head.
- **Ball Point Pens**. The pressure of the ball point pen will scratch the disk surface. Use only felt markers.
- **Heat**. Do not place the disk on or near any heat surface as warping can occur.
- **Power surge**. A power surge protector should be used to avoid loss of data. This is extremely important in certain metropolitan areas of the country where "brown-outs" are common (*Business Computer Systems*, 1982).

Software Theft And Misuse

In a comprehensive article in *Today's Office* dealing with the software theft issue, Jim Seymour states that "vendors like licensing software rather than selling it outright, for that appears to give them greater control over the product's use." The users generally feel that once they have purchased the software, allowances for back-up copies should be granted by the vendor, rather than "blowing up" the program when the user tries to make a copy. "While waiting for order and clarity to come to the statute books, both software vendors and corporate users are finding ways to deal with the question of illegal copying" by drafting site licenses for multiple machine users (agreements allowing the copying and use of programs or large numbers of machines without paying the equivalent of the retail, quantity – one price for each) and various software-protection systems (Seymour, 1984). New policies are being formulated by organizations using computers in terms of employees' use of software, corporate-policy statements and restricting program disks to a limited number of employees to avoid any enfringement violations from occurring.

The Threat From Within

According to Schweitzer in *Computer Crime and Business Information*, "the primary risk to business information today is its theft or misuse in written form by employees," Most information today exists in some tangible form – paper, disks, microfilm, etc. – and is, therefore, quite portable. The ready availability of copying machines make the task of running an extra copy quite simple. Many times, employees run copies merely as a back-up but, all too often, illegal copies are made and used for illegal purposes or financial gain. Establishing a formal corporate policy on employee ethics and loyalty should become a part of the organization's security program. Many employees may not fully understand how vulnerable information becomes when multiple copies are run and left to collect dust on file cabinets, desks and easily accessed by those intent on misusing that information (Schweitzer, p. 14).

Physical Security

The ideal location for storing the microcomputer is in a locked room, an area not accessible to all employees. The layout of the office or the sheer number of micros in an organization may prohibit this type of security, however. In that case, securing micros at the users' desks is the next option. Susan Foster in *Computer Decisions* (July, 1983) suggests the following:

- Use of computer tables with lockable covers that enclose the entire system, allowing for initiating dust protection as well as physical security.

- Bolting the CPU to the desk and limiting access by a key to unlock the case.

- Develop a back-up plan and recovery procedures.

- Provide rules and facilities to protect sensitive information in shared environments.

- Locate off-premises storage for critical data.

- Adopt standard naming conventions for all data and files to avoid "losing" data when someone cannot remember a file name.

- In unsecured areas, provide a means to protect the computer and its components from unauthorized use or theft.

- If the computer is connected to dial-up communication facilities, ensure that sensitive data is protected from unauthorized users.

Encryption And Passwords

A very effective method of limiting access to only authorized personnel is encryption, a method of garbling and compressing data to make it readable to anyone with a translation command code. In a recent article entitled, "Protect Yourself From Crime" in *Business Computer Systems*, the author stated that " . . . until recently (encryption) has been used almost exclusively when information is transmitted to and from remote locations. Encryption is, however, a practical, effective method of safeguarding any important data."

Password protection may also be utilized to limit access only to those users able to supply the requested password. If the user fails after several tries to enter the correct password, the system should shut down. Indexes containing passwords should be kept locked in a separate location away from the worksite and access to the index should be limited. As an additional security measure, passwords should be changed regularly.

Security Solutions

Martin in *Interface Age* (February, 1984) offers ten computer security solutions suggested by Gerald I. Isaacson, a director at the Computer Security Institute in Northborough, Massachusetts:

- Establish formal policies concerning the use of corporate computers – both at the office and at the employee's home.

- Each user must be accountable for the device, the software, and vital information being used.

- Provide facilities for the safe storage of media.

- Each user must be instructed in the minimum care requirements of the computer.

Schweitzer offers a similar listing by stating that "the personal computer user must be required to use all the security features available and must be motivated to follow good security discipline" (p. 116). This means:

- Using passwords of at least six characters in length, not easily guessed by others and changed at least every ninety days.

- Use encryption or file lockwords when a fixed disk is in use. Again, these should not be easily guessable.

- Lock away floppy disks when not in use.

- For high-value information, use encryption when appropriate. Situations where telecommunications is appropriate include strategic planning, funds transfer, product research, financial reporting, and market research strategy applications.

- Avoid printouts where unnecessary and destroy unneeded printouts by shredding or burning. Avoid using the wastebasket for any sensitive information.

- Protect tapes, disks, microfilm, and other documents when enroute or in public places (p. 116-117)

The issues of data security that have plagued the mainframe computer environment for a long time must now be considered in the microcomputer environment as well. Many of the issues, such as personnel selection, disaster and fire protection, user authorization, etc., definitely have a role to play in the micro environment, just as they did with mainframes. The micro environment, at the same time, introduces a new set of problems and considerations that are unique to this new, rapidly advancing technology

We must readjust our "security thinking" to keep pace with all the changes that technological advances introduce and be prepared to apply this new knowledge concerning security and control into our operation so that users are aware of the breaches and accidents that will face them. With knowledge and awareness, we will be ready to face the challenge.

Editor's Note: For more information about this article you can contact: Dr. Karen A. Forcht, Assistant Professor, James Madison University, Department of Information and Decision Sciences, Harrisonburg VA 22807. Phone: 703-433-2545. ■

GLICKMAN REINTRODUCES COMPUTER SECURITY BILL

Representative Dan Glickman (D-Kan.) announced the introduction of a bill aimed at lessening vulnerabilities of Federal computer systems. It would require that each agency provide mandatory, periodic training in computer security awareness and practices. The bill was considered by the full House under suspension of the rules during the last session but, on a vote of 217-206, fell short of the necessary two-thirds majority needed for passage under a special procedure.

Upon reintroduction of the bill on the first day of the 100th Congress, Glickman said, "Since a major definitional problem was recently dealt with in other legislation and because the underlying issue — the poor state of Federal computer security — is still with us, I intend to vigorously pursue passage of this bill. The bill also would overturn a Presidential directive which has placed all security responsibilities within the National Security Agency. For the most part, this should be a civilian — not a military — function.

This legislation is vital when you consider that computers are used by air traffic controllers to help separate air traffic, banks and other financial institutions, agencies which disperse social security and veterans benefits and the Pentagon to store security information. Without proper computer security, I hate to think of the catastrophes that can result."

Joining Glickman as original cosponsors are Governmental Operations Committee Chairman, Jack Brooks (D-Tex.) and ranking minority member Frank Horton (R-N.Y.); Science and Technology Committee members Robert A. Roe (D-N.J.), George Brown (D-Calif.), Doug Walgren (D-Pa.), Sherwood L. Boehlert (R-N.Y.); and Ron Wyden (D-Or.).

Editor's Note: For more information, contact: Cheri Farha, 2435 Rayburn House Office Bldg., Washington, DC 20515. Phone: 202-225-6216. ■

IIA ISSUES STATEMENT OPPOSING DoD INFORMATION RESTRICTIONS

Editor's Note: The following is a statement released by the Information Industry Association.

Recent events suggest that certain persons within the United States government are attempting to restrict or monitor citizen access to unclassified information that is now generally available to the public.

- On October 29, 1986, the President's National Security Advisor issued a new, extremely broad security classification for government information: "sensitive but unclassified information." Implementation of this definition, which includes "human, financial, industrial, agricultural, technological, and law enforcement information," could deny citizens the right to acquire government information which has traditionally been available to the public.

- On November 11, 1986, a senior Department of Defense official stated that privately owned, unclassified electronic databases would be reviewed for "sensitive but unclassified information" and that access to these databases may be restricted or systems installed to monitor who uses them. Such actions could severely limit the information available to citizens, have a chilling effect upon those who wish to acquire information, and curtail the ability of U.S. information companies to do business.

- Over the last few months, representatives from the Department of Defense, Central Intelligence Agency and Federal Bureau of Investigation have been visiting private information companies to ask ques-

We must readjust our "security thinking" to keep pace with all the changes that technological advances introduce and be prepared to apply this new knowledge concerning security and control into our operation so that users are aware of the breaches and accidents that will face them. With knowledge and awareness, we will be ready to face the challenge.

Editor's Note: For more information about this article you can contact: Dr. Karen A. Forcht, Assistant Professor, James Madison University, Department of Information and Decision Sciences, Harrisonburg VA 22807. Phone: 703-433-2545. ■

GLICKMAN REINTRODUCES COMPUTER SECURITY BILL

Representative Dan Glickman (D-Kan.) announced the introduction of a bill aimed at lessening vulnerabilities of Federal computer systems. It would require that each agency provide mandatory, periodic training in computer security awareness and practices. The bill was considered by the full House under suspension of the rules during the last session but, on a vote of 217-206, fell short of the necessary two-thirds majority needed for passage under a special procedure.

Upon reintroduction of the bill on the first day of the 100th Congress, Glickman said, "Since a major definitional problem was recently dealt with in other legislation and because the underlying issue — the poor state of Federal computer security — is still with us, I intend to vigorously pursue passage of this bill. The bill also would overturn a Presidential directive which has placed all security responsibilities within the National Security Agency. For the most part, this should be a civilian — not a military — function.

This legislation is vital when you consider that computers are used by air traffic controllers to help separate air traffic, banks and other financial institutions, agencies which disperse social security and veterans benefits and the Pentagon to store security information. Without proper computer security, I hate to think of the catastrophes that can result."

Joining Glickman as original cosponsors are Governmental Operations Committee Chairman, Jack Brooks (D-Tex.) and ranking minority member Frank Horton (R-N.Y.); Science and Technology Committee members Robert A. Roe (D-N.J.), George Brown (D-Calif.), Doug Walgren (D-Pa.), Sherwood L. Boehlert (R-N.Y.); and Ron Wyden (D-Or.).

Editor's Note: For more information, contact: Cheri Farha, 2435 Rayburn House Office Bldg., Washington, DC 20515. Phone: 202-225-6216. ■

IIA ISSUES STATEMENT OPPOSING DoD INFORMATION RESTRICTIONS

Editor's Note: The following is a statement released by the Information Industry Association.

Recent events suggest that certain persons within the United States government are attempting to restrict or monitor citizen access to unclassified information that is now generally available to the public.

- On October 29, 1986, the President's National Security Advisor issued a new, extremely broad security classification for government information: "sensitive but unclassified information." Implementation of this definition, which includes "human, financial, industrial, agricultural, technological, and law enforcement information," could deny citizens the right to acquire government information which has traditionally been available to the public.

- On November 11, 1986, a senior Department of Defense official stated that privately owned, unclassified electronic databases would be reviewed for "sensitive but unclassified information" and that access to these databases may be restricted or systems installed to monitor who uses them. Such actions could severely limit the information available to citizens, have a chilling effect upon those who wish to acquire information, and curtail the ability of U.S. information companies to do business.

- Over the last few months, representatives from the Department of Defense, Central Intelligence Agency and Federal Bureau of Investigation have been visiting private information companies to ask ques-

tions about who is using their information and for what purposes. It appears that the national security community is attempting to intimidate information companies into restricting access to their information or policing who uses it.

These government actions appear to be in response to concerns that foreign access to information, especially where available through new technologies such as on-line databases, is a potential threat to United States national security. Although the basis for these concerns has not been publicly documented, it is apparent that the information in question is unclassified government and private sector information that any citizen can easily and legally obtain by going to a public library. Should there be legitimate national security concerns about foreign access to information, the protection of such information must be addressed in accordance with the democratic process of checks and balances. Individual government officials cannot be permitted to restrict the right of citizens to create, acquire, use, and disseminate information in a manner that contravenes Constitutional and statutory law.

The United States information industry is seriously concerned that certain individuals or organizations of the United States government are, in a manner that is inconsistent with democratic traditions, attempting to regulate or restrict access to unclassified government and privately-owned information now generally available to the public. Accordingly, the Board of Directors of the Information Industry Association adopted the following set of principles at its December 16, 1986 meeting.

- The United States democracy is an open society in which freedom of speech, freedom of the press, and the right of citizens to create, acquire, use and disseminate information are fundamental rights.

- The traditional United States policy of not restricting foreign access to information that is generally available to the public is sound. Any change in that policy would inevitably result in limiting the ability of U.S. citizens and allies to acquire information.

- Citizens and organizations should be free to acquire, use, and disseminate information generally available to the public without fear of government interference or monitoring.

- The unimpeded flow of information and the innovative use of new technologies contribute to the nation's technological, economic and political strength, thereby maintaining the United States position as a world leader.

In accordance with these principles, the Information Industry Association has adopted the following position:

- United States policy should continue to foster openness and the unimpeded flow of information. Restrictions imposed on the right of citizens to create, acquire, use, and disseminate information should be the absolute minimum necessary to protect national security.

- National security is best protected by using the long existing classification system to ensure that government information vital to the nation's security is not released to the public. The concept of "sensitive but classified information" provides an unchecked hunting license for governmental officials to deny citizens access to information and must be rejected.

- The security classification system should not be used to unnecessarily restrict public access to government information: the decision to classify information should weigh national security interests against the right of the public to acquire information.

- Classification of information for national security purposes should not be based upon the media in which the information is available. Information which is unclassified and available to the general public, such as in print through a library, must not be restricted or classified when it enters an electronic database.

- Once government information is released to the public, the government should not restrict the right of citizens to access

such information or require information providers to monitor who uses the information.

- If Department of Defense and other government agencies are concerned that public access to unclassified information is detrimental to the national security, they should make public the full bases of these concerns.

- All information users must be assured that their privacy and confidentiality are fully protected in accordance with law and the highest possible ethical business practices. Authors, publishers and other information producers and providers must be assured that their creation of information, or their use and dissemination of unclassified government information, does not subject them to government censorship.

- Government agencies should not attempt to dissuade information companies from legal business practices through intimidation or coercion.

The United States has spent 200 years in achieving a balance between natoinal security interests and the right of citizens to create, acquire, use, and disseminate information. Changes in this balance should take place in an open forum in which all citizens have an opportunity to participate. Such a forum is the Congress of the United States.

Editor's Note: For more information, contact: Paul G. Zurkowski, President, Information Industry Association, 555 New Jersey Ave., N.W., Suite 800, Washington, DC 20001. Phone: 202-639-8262. ■

MAJOR FIRMS JOIN A NEW INSTITUTE TO PROTECT INFORMATION ASSETS

Some of the largest companies in the world are participating in a new institute dedicated to protecting their information assets.

"Information is a valuable and fragile strategic asset that must be protected, especially in today's automated environment," said Donn B. Parker, an internationally known expert on information security at SRI International.

Parker worked with more than a dozen major firms over the past three years to develop the International Information Integrity Institute (I-4), which began operations in December.

Some of the key services being offered by I-4 are: reporting on the types and nature of information losses, interaction with Federal agencies charged with computer security functions, and documentation of baselines of generally accepted security controls and practices.

Charter members include 3M, Aetna Life & Casualty, Amoco, Chemical Bank, Comdisco, Digital Equipment Corp., The Hartford Insurance Group, Honeywell, IBM, ICL, NCR Corp., Sears Roebuck and Company, UCCEL (formerly SKK), and Wells Fargo Bank.

U.S. government agencies that also will interact with I-4 include two branches of the National Security Agency — the National Computer Security Center and the National Information Security Assessment Center — as well as the National Bureau of Standards' Institute of Computer Sciences and Technology, in the U.S. Department of Commerce.

SRI, one of the world's largest contract research and consulting organizations, has conducted security reviews for more than 85 companies worldwide since 1970. This experience, plus SRI's file of over 1,600 computer abuse cases and extensive research into computer security, will form the foundation for providing services in the broader area of information integrity.

With the proliferation of electronic funds transfer, electronic and voice mail, microcomputers, and computer networks, greater protection of electronically stored and transmitted information is essential. But, "computer and communications security is not enough," according to Parker.

"Business organizations must be concerned with the broader concept of information integrity, which means maintaining information in good condition and safeguarding it not only from unauthorized appropriation and use, but also from such

things as accidental modification. misplacement. replacement. and destruction."

Parker pointed out that because of recent legislation and insurance considerations. corporate officers and board members must be even more diligent in exercising due care in protecting corporate assets. including not only the corporation's sensitive records. but also the records of its customers. I-4 wil help executives meet the functional. legal and insurance standards of due care.

In addition to an advisory hotline and reporting on types and nature of losses stemming from breaches of security. I-4 members will get reports on new SRI research ranging from technical topics. such as intrusion detection and encryption. to management issues. such as expenditures for information security.

The membership fee also includes two-day. on-site clinics. forums. and short term guest research fellowships at SRI.

The International Information Integrity Institute will be headquartered at SRI's Menlo Park. Calif., offices and will also be supported through SRI's London. Paris. and Far East offices.

Editor's Note: For further information, contact: Bruce Baker, SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025. Phone: 415-859-4729. ■

FAMED COMPUTER HACKER STILL BEING SOUGHT

Bill Landreth has not been seen or heard from since early one September morning. when he had pushed himself away from his IBM-PC computer — in mid-sentence — and walked out of the front door of a friend's house in Escondido. Calif.

For the authorities this might just be another routine missing person. But Landreth is not just an ordinary missing person. he is the famed computer hacker known as the "Cracker."

Landreth was convicted in Federal court in 1984 for breaking into some of the most secure computer systems in the United States. including GTE Telemail's electronic mailbox in Vienna. Va., where he allegedly peeped at NASA and Department of Defense computer correspondence. He also pleaded guilty to sharing his secrets within a network of other computer hackers known as The Inner Circle. He was known to the group only as the "Cracker."

He was placed on three years probation. Now his probation officer is wondering where he is.

His literary agent. Bill Gladstone is also wondering where he is. Landreth. the author. who has already cashed in on the successful publication of one book on computer hacking. is overdue with the manuscript of a second book.

Some people think Landreth. 21. has committed suicide. They are convinced of this because of a rambling eight-page letter he wrote over the summer.

The letter. typed into his computer. then printed out and left in his room for someone to discover. discussed the evolution of mankind. prospects for man's immortality. the defeat of the aging process. nuclear war. communism vs capitalism. society's greed. the purpose of life. computers becoming more creative than man and finally — suicide.

The last page of the letter reads:

" . . . I was bored in school. bored traveling around the country. bored getting raided by the FBI. bored in prison. bored writing books. bored being bored. I will probably be bored dead. but this is my risk to take."

"Since writing the above. my plans have changed slightly. I have. in the past few months. been kept busy dispersing the moneys in my bank account. and at this moment it is fairly low. Don't get me wrong: I still have plenty to live on . . . and I have about an additional $1.000 in checks that I have not bothered to cash. But the point is that I am going to take this money I have left in the bank (my liquid assets) and make a final attempt at making my life worthy. It will be a short attempt. and I do suspect that if it works out that none of my current friends will know me then. If it doesn't work out. the news of my death will probably get around. (I won't try to hide it). . . ."

Landreth also said the "idea is that I will commit suicide sometime around my 22nd

birthday . . ." His birthday was Dec. 26 and his best friend, among others, is not counting on seeing him again.

"We used to joke about what you could learn about life, especially since if you don't believe in a god, then there's not much point to life," said Tom Anderson, 16, a senior at a local high school in Escondido. Anderson has also been convicted in Federal court of computer hacking and placed on probation.

Anderson was the last person to see Landreth. It was around Sept. 25 — he does not remember exactly. Landreth had spent a week living at Anderson's home so the two could share Landreth's computer. Anderson's IBM-PC had been confiscated by authorities, and he wanted to complete work on his own book. Anderson said that he and Landreth were also working on a proposal for a movie about their hacking exploits.

"He started to write the proposal for it on the computer and I went to take a shower," Anderson said. "When I came out, he was gone. The proposal was in midsentence. And I haven't seen him since."

Anderson said he was not initially concerned about his friend's disappearance. During the summer, Landreth had gone to Mexico for three weeks without telling anyone — including friends he had seen the night before.

He became concerned when Landreth had failed to show up for a speaking engagement with a group of auditors in Ohio Oct. 1. Landreth would have received $1,000 plus expenses.

The San Diego, Calif., Police Department began investigating Landreth's disappearance after friends filed a missing persons report in mid-October. But field representative Camille Sherrill said she turned the case over to Federal authorities after she learned that Landreth was in violation of his probation. A Federal bench warrant was issued for his arrest and he is now, among others, being sought by the U.S. Marshals.

Editor's Note: This is a rewrite of an article which appeared in the ***Houston Chronicle.*** ■

CALENDAR OF EVENTS

Feb. 20-22 — The Electronics & Computer Showcase Spectacular, Jacksonville, FL. Fee: $4 admission charge at the door. Contact: Great Southern Computer & Electronics Show, P.O. Box 655, Jacksonville, FL 32201. Phone: 904-743-8000.

Feb. 26-28 — Expo South '87, Orlando, FL. Fee: $10 admission to exhibits; $325 for six session package of seminar programs. Contact: Cahners Exposition Group, Cahners Plaza, 1350 E. Touhy Ave., P.O. Box 5060, Des Plaines, IL 60017-5060. Phone: 312-299-9311. International Telex: 82882 CEG CHGO. US Telex: 256148 CEGCGO DSP.

March 4-6 — Securicom '87, Paris, France. Fee: FF 7 116. Contact: Securicom-Sedep, 8, rue de la Michodiere, 75002 Paris, France. Phone: (1) 47.42.41.00 + Telex 250303 PUBLIX X PARIS-ATTN SEDEP.

March 9-10 — Automated Manufacturing: Computers, Communications & Controls, St. Petersburg, FL. Contact: Eleanor Bernet, Industry Representative, Frost & Sullivan, Inc., 106 Fulton St., New York NY 10038. Phone: 212-233-1080.

March 9-10 — Knowledge-Based Artificial Intelligence, Los Angeles, CA. Fee: $1195. Contact: Integrated Computer Systems, 5800 Hannum Ave., P.O. Box 3614, Culver City, CA 92031. Phone: 800-421-8166, or 213-417-8888. Telex 4995168. Also offered other dates and places.

March 23-27 — EDPAF 17th Conference on Computer Audit, Control and Security, Boston, MA. Contact: Registrar, EDP Auditors Association, P.O. Box 88180, 455 Kehoe Blvd., No. 106, Carol Stream, IL 60188-0180. Phone: 312-653-0950. Telex 280 427 EDP CGO UD. ■

FEDERAL, STATE OFFICIALS LAUNCH JOINT CAMPAIGN NATIONALLY AGAINST TELEMARKETING FRAUD

Federal and state officials announced on Jan. 15 that they are launching a joint campaign against telemarketing fraud — the deceptive peddling of goods and services over the telephone.

Saying con artists swindle consumers out of $1 billion per year, Federal Trade Commission (FTC) Chairman Daniel Oliver said the primary weapon against this kind of fraud will be an information-sharing agreement between the Federal Government and the National Association of Attorneys General (NAAG).

"To accomplish this goal," Oliver told a news conference in Washington, "we are establishing an information clearinghouse on telemarketing fraud."

The efforts also are to include joint Federal-state investigations. the sharing of technical expertise and litigation resources and a campaign to educate consumers on the dangers of telemarketing fraud.

"If (a telephone solicitation) sounds too good to be true," warned Iowa Attorney General Tom Miller, "it is too good to be true."

Miller added the purpose of the crackdown is to "frustrate people perpetrating this fraud . . . and we want to give them a dose of deterrence."

Telemarketing fraud — the peddling of everything from gemstones to oil and gas leases and cellular telephone systems to rare coins and countless other items — has become a big business largely due to modern technology, said Arkansas Attorney General Steve Clark, who also serves as president of NAAG.

"The ease of securing wide area telephone service (WATS) and the relatively low costs to maintain them has caused a proliferation of WATS-line hustlers," said Clark. "For the con artist, it has the advantage of reaching large numbers of people and being difficult to trace."

Law enforcement officials said it is often difficult to prosecute "WATS-line hustlers" because they can easily move their operations to new locations in different states under new names.

Up until now, the FTC said it has sued operators of telemarketing fraud who collectively have made sales of about $590 million to more than 72,000 consumers.

Oliver also announced the FTC on Jan. 15 began mailing $2.7 million in refunds to consumers who were victimized by Leland Industries, Inc., a Texas-based firm. The Commission had charged that Leland falsely claimed in telephone calls to potential clients that they were likely to win highly valuable oil and gas leases. ■

LOW COST PC SECURITY SYSTEM UNVEILED

A-O Electronics, Inc., has introduced the X-LOCK 50, an inexpensive PC security system which prohibits unauthorized computer use and protects confidential files.

Consisting of an internal half-card and software diskette, the X-LOCK 50 prevents unauthorized use of a computer by limiting access only to approved personnel. The X-LOCK 50 also features high-speed data encryption which allows selected files or entire disks to be encrypted using the DES encryption algorithm. The PC security system is now available from A-O Electronics for only $275 with quantity discounts for volume users.

The system accommodates up to 180 user accounts stored in fail-safe circuitry which protects data even if the X-LOCK is removed or damaged. Each user account consists of the user's name and a one-to-16 character password, which can be easily altered at any time. A system "super user" maintains ultimate control over the system, assigning passwords and adding or deleting account.

Once a file or disk has been encrypted using the X-LOCK 50, it is impossible for any unauthorized user to read or decipher the information. However, the X-LOCK 50 can quickly decrypt coded files for authorized users.

According to David Brewster, Vice President of Marketing for A-O Electronics, "Once the user has successfully logged on with his name and password, X-LOCK 50 is completely transparent to any other software application. In fact, it is not even necessary to log off X-LOCK 50 before logging off the computer."

Other features of the X-LOCK 50 include self-diagnostic capabilities and the ability to automatically lock up the computer after several unauthorized attempts to access the system.

The firm also produces the X-LOCK 100, a larger security and resource management system for the IBM PC and compatibles which sells for $495.

Editor's Note: For more information about the X-LOCK 50 or any other product, contact A-O Electronics, 2137 Flintstone Drive, Tucker, GA 30084. Phone: 404-491-8044. ■